MAANPUOLUSTUSKORKEAKOULU

YHTEISKUNNAN TOIMINTA UUSIA UHKIA VASTAAN

Pro gradu -tutkielma

Yliluutnantti
Mika Isometsä

Sotatieteiden maisterikurssi 2
Maasotalinja

Huhtikuu 2013

MAANPUOLUSTUSKORKEAKOULU

Kurssi	**Linja**
Sotatieteiden maisterikurssi 2	Maasotalinja
Tekijä	
Yliluutnantti Mika Isometsä	
Tutkielman nimi	
YHTEISKUNNAN TOIMINTA UUSIA UHKIA VASTAAN	
Oppiaine johon työ liittyy	**Säilytyspaikka**
Johtaminen	Kurssikirjasto (MPKK:n kirjasto)
Aika	
Huhtikuu 2013	Tekstisivuja 70 Liitesivuja

TIIVISTELMÄ

Tutkimuksessa tutkittiin miten suomalainen yhteiskunta toimii uusia uhkia vastaan. Tutkimuksen rajauksena käytettiin uhkana ainoastaan kyberuhkaa, mitä vastaan yhteiskunnan toimia tutkittiin. Kyberuhka on tietoyhteiskunnan uusin uhkatekijä, joka on noussut voimakkaasti vanhojen uhkakuvien rinnalle. Tutkimus on ajankohtainen, koska Suomi on saanut ensimmäisen kansallisen kyberstrategian tammikuussa 2013. Kyberstrategian antamia suuntaviivoja ei ole vielä ehditty saattaa kunnolla käytäntöön, mutta kyberstrategia on osoitus yhteiskunnan toimista. Kyberturvallisuus on ollut esillä mediassa voimakkaasti viime aikoina erilaisten palvelunestohyökkäysten ja varautumistoimenpiteiden vuoksi.

Tutkimus on toteutettu laadullisena, teoriaohjaavan sisällönanalyysin avulla tehtynä tutkimuksena, jossa uhkana toimi kyberuhka ja viitekehyksenä toimi suomalainen yhteiskunta. Tutkimuksen tiedonkeruumenetelmänä oli tiedonhankinta julkisista kirjallisista lähteistä, asiakirjoista ja internet-lähteistä.

Tutkimuksessa on määritettyjen tutkimuskysymysten kautta vastattu keskeiseen tutkimusongelmaan, jossa on selvitetty miten uudet uhkat vaikuttavat yhteiskunnan varautumiseen.

Keskeisen tutkimusongelman selvittämistä varten tutkimuksen pääkysymykseni oli miten yhteiskunta varautuu uusiin uhkiin? Saavuttaakseni kattavan vastauksen määritin päätutkimuskysymystä tukemaan alatutkimuskysymyksiä jotka olivat:

Mitä ovat uudet uhkat ja miten kyberturvallisuusstrategia huomio kyberuhkan?

Tutkimus on osoittanut, että suomalainen yhteiskunta on ottanut selkeän askeleen varautumis-

toimenpiteissä uusia uhkia vastaan. Oma kansallinen kyberturvallisuusstrategia on omalta osaltaan voimakas kannanotto ja teko toimissa uusia uhkia vastaan. Kyberturvallisuusstrategia ei anna valmiita toimintamalleja kuinka erilaisissa tilanteissa toimitaan, mutta sen avulla määritetään toimivaltuuksia ja toimijoita, jotka toimivat tilanteen niin vaatiessa. Suomeen perustettavan kyberturvallisuuskeskuksen toiminta on tärkeässä osassa yhteiskunnan toimia varten. Kyberturvallisuuskeskuksesta on tarkoitus muodostaan järjestelmän ydin, joka koordinoi kaikkea kyberturvallisuuteen liittyviä asioita Suomessa. Vahvuutena tulevalla keskuksella on sen luominen viestintäviraston luomalle CERT-FI -pohjalle, joten toimintaa ei tarvitse kehittää alkutekijöistä.

Tutkimuksesta käy ilmi, että mikään keskus ei yksin kykene toimimaan, vaan se vaatii vahvasti yhteistyötä yksityisen ja julkisen sektorin välillä. Kyberturvallisuuskeskuksen tehtävänä onkin vakuuttaa eri tahot kyberturvallisuuden tärkeydestä.

Tutkimus on mielestäni osoittanut aihetta jatkotutkimukselle, jossa tutkittaisin yksittäisen kansalaisen toiminnan vaikutusta kyberturvallisuuteen ja kuinka kansalaisen ymmärrystä asian tärkeydestä saataisiin lisättyä.

AVAINSANAT

kyberturvallisuus, kyberturvallisuusstrategia, palvelunestohyökkäys, vakoiluohjelmat, tietokonevirukset, suojautuminen, kyberuhka

YHTEISKUNNAN TOIMINTA UUSIA UHKIA VASTAAN

YHTEISKUNNAN TOIMINTA UUSIA UHKIA VASTAAN

1. JOHDANTO

1.1 Johdatus tutkimusaiheeseen

Yhteiskunta ei ole vielä riittävästi valmistautunut perinteisistä sotilaallisista ja ympäristön poikkeuksista aiheutuvien kriisitilanteiden ratkaisuihin. Enää ei pelkkä suoranainen sotilaallinen toimi ole ainoa yhteiskuntaa uhkaava tekijä. Yhteiskunnan teknologistuminen on tuonut tullessaan uusia mahdollisia uhkatekijöitä. Nyt uhkakuvien määrittely on muodostunut vaikeaksi. Maailma on muuttunut voimakkaasti digitaalisen suuntaan ja yhteiskunta tarvitsee voimakkaasti tätä digitaalista apua ollakseen toimiva yhteiskunta. Tietokoneet ohjaavat tavalla tai toisella lähes kaikkea tärkeää infrastruktuurista, maanpuolustuksesta ja tiedonvälityksestä alkaen. Mikäli virtuaalista maailmaa häiritään jotenkin meille epäedullisella keinolla, sen seuraukset voivat vaikuttaa tuhoisasti yhteiskuntaamme.

Limnéll toteaa kirjassaan Suomen uhkakuvapolitiikka 2000-luvun alussa julkisten uhkakuvien rakentuvan valtiossa poliittisessa vuorovaikutuksessa toimijoiden välillä ja valtion ulkoisten toimijoiden ilmentämät uhkakuvat yhdistyvät läheisesti ulkoisiin toimijoihin. Uhkakuvien määrittely on muodostunut avoimeksi ja suurelle yleisölle on annettu mahdollisuus seurata keskustelua uhkakuvien muodostumisesta.

Kylmän sodan (1945–1990) aikana suomalaista yhteiskuntaa johdettiin vahvasti presidenttijohtoisesti, turvallisuus- ja uhkakuvakeskustelut käytiin hyvin pienellä piirillä. Uhkakuvien määrittelyssä oli vahvasti painotettuna sotilaallinen luonne. Julkinen uhkakuva oli todennäköisesti eri kuin mihin todellisuudessa varauduttiin. Uhkakuvien arvioinnissa pääpaino oli sotilaallisilla kysymyksillä ja voimapolitiikalla. (Limnéll 2009, 4-5).

Tilanne muuttui kylmän sodan päättymisen jälkeen. Neuvostoliiton kanssa tehty YYA-sopimus raukesi ja suomen liittyminen EU:n jäseneksi muutti suomalaista turvallisuuspolitiikan keskusteluilmapiiriä. Keskusteluissa voimistuivat uudet uhkat, laaja turvallisuuskäsite ja sotilaallinen uhka koettiin pienemmässä merkityksessä. Uhkat nähtiin laajemmin ja ne siirtyivät ajallisesti ja maantieteellisesti etäämmälle. (Limnéll 2009, 5).

Sotilaallisten uhkakuvien rinnalle on noussut erilaisia epäsymmetrisiä uhkia, joista keskeisin uhka on terrorismi. Vastustajana ei siis toimi perinteinen ja selkeä vihollisarmeija. Uusien uhkien taustalla ovat yhteiskunnan vahingoittamiseen tähtäävä toiminta tai uhkaaminen. Uhkaajana ei välttämättä ole valtio vaan sen takana voi olla myös ei-valtiollinen toimija. (Turvallisuuspoliittinen seurantaryhmä 2008, 18).

Globalisaation lisääntyminen vaikuttaa valtion johtamiseen ja puolustusjärjestelmän turvaamisen suunnitteluun. Globalisaatiolla tarkoitetaan laajaa yhteiskunnallista muutosta, joka ilmenee keskinäisriippuvuuden kasvuna ja se syventää kansainvälistä yhteistyötä. Maailmanlaajuinen verkottuminen mahdollistaa tiedon, ajatusten, palvelujen, tavaroiden, pääoman ja ihmisten liikkumisen esteettömämmin. Maailmantalous on kehittynyt nopeaa vauhtia, sen myötä kehitysongelmat ovat kärjistyneet. Suomi on hyötynyt globalisaatioprosessista, joka tarjoaa mahdollisuuksia. Mahdollisuuksien myötä ovat lisääntyneet haasteet, joihin meidän on kyettävä vastaamaan. (Turvallisuuspoliittinen seurantaryhmä 2008, 12-13).

Lisääntynyt maailmanlaajuinen yhteistyö on lisännyt Suomea kohtaan maailmanlaajuisia epäsymmetrisiä uhkia. Näistä keskeisin uhka on terrorismi, erilaisine muotoineen. (Turvallisuuspoliittinen seurantaryhmä 2008, 18) Uutena uhkamuotona tunnetaan kyberuhka, joka kohdistuu tietoyhteiskuntaan sekä informaatioympäristöön. Aikaisemmin ei ole ollut samankaltaista tietoyhteiskuntaa ja sen myötä on perinteisten uhkakuvien rinnalla tullut uutena niin sanottu kyberuhka. Se ei poista perinteistä sotilaallista voimankäyttöä eikä sulje sen käyttöä pois. Kyberuhkat mielletään rajoja ylittäväksi, jotka voivat sisältyä poliittisiin, taloudellisiin, sotilaallisiin, kaupallisiin, käytännössä kaikille aloille tietoyhteiskunnassa. Uusien uhkien ja kyberuhkien merkittävyydestä kertoo, että NATO:n strategisen konseptin valmistelussa ovat korostuneen kyberuhkat ja terrorismi (Puheloinen 8.11.2010).

Kyberuhkaa pidetään nykypäivänä yhtenä keskeisimpänä uhkana kansalliselle turvallisuudelle ja kansantaloudelle. 1980- ja 1990-luvun harrastuspohjaisesta toiminnasta, jossa teknisesti taitavat henkilöt mittelivät taidoillaan toisiaan vastaan, on tilanne muuttunut. 1990-luvun ja 2000-luvun alussa tilanne muuttui merkittävästi. Rikolliset havaitsivat tietoverkkorikollisuudessa valtavan potentiaalin. Terroristijärjestöt ja muut ääriryhmittymät löysivät mahdollisuutensa kyberavaruudesta. Kyberavaruutta ei ole toistaiseksi hyödynnetty samaan aikaan ja samanlaisin vaikutuksin kuin perinteinen pommi, mutta tähän on jokaisen kansakunnan syytä varautua. Toistaiseksi kyberavaruus on ollut keino häiritä erilaisin keinoin kansakuntien toimintaa (Candolin, 2012, 5-6).

Kyberuhka on tällä hetkellä hyvin ajankohtainen tutkimuskohde, koska se koskettaa meitä kaikkia tietokoneen käyttäjiä ja Suomen kansalaisia. Kyberuhka valittiin tutkimuskohteeksi, koska kyber vaikuttaa jokaisen kansalaisen arkeen. Suomelle on laadittu ensimmäinen kyberturvallisuus strategia, joka on julkaistu tammikuussa 2013. Strategiassa on otettu huomioon yksittäisen ihmisen turvattomuus kybertoimintaympäristössä sekä siinä on huomioitu kyber aiempaa vaarallisemmaksi koko yhteiskunnalle. Tämä tekee tutkimuksesta vielä ajankohtaisemman. Viime aikoina kyberasiat ovat saaneet television ja sanomalehtien kautta runsaasti näkyvyyttä. Talouselämän julkaisu Forbes-lehdessä oli 2012 toukokuun 12. päivän numerossa Tomer Tellerin artikkeli: The biggest cybersecurity threats of 2013. Artikkelissa käsiteltiin tietoverkkohyökkäyksien muuttuneita toimintatapoja ja pohdittiin niiden havaitsemisen vaikeutumista. Tuorein uutisointi verkkohyökkäyksistä on maaliskuulta 2013, jossa CERT-FI ilmoitti tiedotteessaan Spamhaus-palvelunestohyökkäyksistä. Tässä hyökkäyksessä käytettiin hyväksi nimipalvelimia. Tapauksesta uutisoi myös Iltalehti 28.3.2013.

Tutkimus on siis aiheellinen ajankohtaisuutensa vuoksi ja kyberuhkat ovat globaali uhka, joka vaikuttaa Suomessakin meihin kaikkiin. Iskun ei välttämättä tarvitse kohdistua suoraan Suomeen vaan välilliset vaikutukset voivat rantautua tänne meillekin. Pahimmillaan iskun vaikutukset lamaannuttavat yhteiskunnalle kriittisiä toimintoja, kuten maksujärjestelmiä sekä puolustusvoimien toimintoja. Kyberuhka otetaankin huomioon mahdollisena nykyaikaisen sodankäynnin muotona.

1.2 Tutkimuskysymykset ja tutkittavan aiheen rajaus

Tutkimuksen päätehtävänä on tutkia miten uudet uhkat vaikuttavat yhteiskunnan varautumiseen?
Pääkysymyksenä on, miten yhteiskunta varautuu uusiin uhkiin?
Pääkysymyksen vastaamista tuetaan alatutkimuskysymyksillä:
Mitä ovat uudet uhkat?
Miten kyberturvallisuusstrategia huomioi kyberuhkan?

Tämä tutkielma käsittelee suomalaisen yhteiskunnan toimintaa uusien uhkien varalta. Yhteiskunnan turvallisuusstrategia on määritellyt Valtioneuvoston periaatepäätöksellä 16.12.2010 yhteiskunnan uhkamalleiksi erilaisia uhkia. Näitä uhkia ovat muun muassa:
– voimahuollon vakavat häiriöt
– tietoliikenteen ja tietojärjestelmien vakavat häiriöt – kyberuhkat
– kuljetuslogistiikan vakavat häiriöt
– yhdyskuntatekniikan vakavat häiriöt,
– elintarvikehuollon vakavat häiriöt
– rahoitus- ja maksujärjestelmän vakavat häiriöt
– julkisen talouden rahoituksen saatavuuden häiriintyminen
– väestön terveyden ja hyvinvoinnin vakavat häiriöt
– suuronnettomuudet, luonnon ääri-ilmiöt, ympäristöuhkat
– terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus
– rajaturvallisuuden vakavat häiriöt
– poliittinen, taloudellinen ja sotilaallinen painostus sekä
– sotilaallisen voiman käyttö.

Tässä tutkimuksessa keskitytään käsittelemään uusia uhkia ja niistä vain kyberuhkaa sen eri ilmenemismuodoissa, muut tunnetut uhkat rajataan tästä tutkimuksesta pois. Rajauksella mahdollistetaan keskittyminen kyberuhkan moninaisuuteen. Kyberuhka on itsessään todella laaja ja vieläpä vaikeasti hahmotettava kokonaisuus. Kyberuhkaa käsitellään suomalaisen yhteiskunnan näkökulmasta, mutta on huomioitava, että puhuttaessa kyberista, uhka on aina globaali ja tämän vuoksi se ei noudata valtakunnan rajoja. Tämä tutkimus perustuu julkisiin lähteisiin, koska niitä oli runsaasti saatavilla.

1.3 Aiemmat aiheeseen liittyvät keskeiset tutkimukset

Keskeiset kyberaiheisiin liittyvät tutkimukset ovat muun muassa liittyneet seuraaviin aiheisiin, kuten palvelunestohyökkäyksiin, uhkakuvien erilaisiin tarkasteluihin ja kybertuvallisuutta vaarantaviin tekijöihin.

Limnéll Jarmo on todennut kirjassaan Suomen uhkakuvapolitiikka 2000-luvun alussa, että Suomen uhkakuviin tehtyjä tutkimuksia on vähän, jotka on laadittu kylmän sodan jälkeen. Tutkimukset ovat keskittyneet lähinnä sotilaallisen uhkakuvien tai yksittäisten uhkakuvatekijäkokonaisuuksien tarkasteluun.

Björkman Jyri on tehnyt tutkimuksen Haaga-Helia ammattikorkeakoulussa vuonna 2010 Palvelunestohyökkäykset ja niiltä suojautuminen. Hänen tutkimuksessaan selvitettiin millaisia palvelunestohyökkäyksiä voidaan tehdä ja kuinka niiltä voidaan suojautua. Lisäksi hän pyrki tutkimaan miksi palvelunestohyökkäyksiä ylipäätään tehdään.

Satakunnan Ammattikorkeakoulussa Sillberg Risto on tehnyt opinnäytetyön 2008 Tietoverkkoon tunkeutumisen havainnointi snortin avulla. Hänen opinnäytetyössään tutkittiin kuinka yleisiä palvelunestohyökkäykset ovat ja kuinka tunkeutumisen havaitsemisjärjestelmät toimivat. Hänen opinnäytetyönsä on tekninen ja keskittyy tietoverkkojen tietoturvariskeihin.

Hagestam Axel on tehnyt julkaisun CIP – Kriittisen infrastruktuurin turvaaminen. Hänen raportissaan tarkastellaan länsimaiden kriittisen infrastruktuurin luokittelua ja mitä suunnitelmia sen suojaamiseksi on sekä mitkä tekijät ovat vaikuttaneet suunnitelmien syntyyn. Raportti perustuu yhteiskunnan kriittisen infrastruktuurin nousemiseen länsimaissa turvallisuusuhkien ja tietoyhteiskuntien kehityksen myötä keskeiseen asemaan.

Koskinen Jukka on toimittanut seminaariraportin Palvelunestohyökkäyksen havaitseminen ja torjuminen. Kyseinen dokumentti on editoitu Tampereen teknillisen yliopiston kurssin seminaarikirjoitelmista keväällä 2005. Raportissa avataan palvelunestohyökkäyksien historiaa sekä keinoja millä palvelunestohyökkäyksiä suoritetaan ja kuinka niitä saadaan torjutuksi.
Pullinen Mika on tehnyt Laurea-ammattikorkeakoulussa opinnäytetyön Kriittisten tietojärjestelmien suojaaminen kyberuhkilta vuonna 2012. Hän tutki työssään kuinka organisoitu kyberhyök-

käys voi vaarantaa kansallisen kriittisen infrastruktuurin turvallisuuden. Hänen työssään pyrittiin löytämään vastaukset mitä olisivat ne kohteet mitkä pitäisi suojata ja miten.

Puhakka Jarkko on tehnyt opinnäytetyön Penetraatiotestaus osana tietoturvan toteutusta. Hänen työnsä on laadittu Jyväskylän ammattikorkeakoulussa vuonna 2012. Opinnäytetyössä tutkitaan penetraatiotestauksen avulla suoritettua jäljittelyä, joita mahdollinen hyökkääjä käyttää pyrkiessään murtautumaan tietoverkkoihin ja järjestelmiin. Testauksen perusteella löydetyt heikot kohdat pystytään parantamaan tietoturvaa paikkaamalla syntyneet aukot.

Kurki Matti on käsitellyt julkaisussaan Tulevaisuuden verkkopalvelut vuonna 2008 Haaga-Helian ammattikorkeakoulussa ihmisille suunnatuista verkkopalveluista. Raportissa käsitellään kuinka ihmiset hyödyntävät palveluita ja kuinka osa palveluista on suunnattu vain ohjelmistojen käyttöön. Hänen tutkimuksensa ei suoranaisesti kosketa kyberia, mutta siinä käsitellään verkkopalveluiden eri muotoja, jotka kuitenkin ovat osa kyberia.

Lukin Kimberly on tehnyt pro gradu – tutkielman Turun yliopistossa 2007 Venäläisten käyttämät tietoverkkosodankäynnin menetelmät. Tutkimuksessa selvitetään Venäjän asevoimien virus- ja ohjelmistosodankäynnin ja sen siviiliversion, hakkerismin erityispiirteitä.

Helin Jukka on tehnyt Lahden ammattikorkeakoulussa 2006 opinnäytetyön Kotikäyttäjän tietoturvasta. Tutkimuksen tarkoituksena on yksinkertaisesti selvittää kuinka yksittäinen tietokone voidaan suojata ja mitä ovat riskit, jotka uhkaavat tietokonetta.

Kajaanin ammattikorkeakoulussa on tehty opinnäytetyö Palvelunestohyökkäykset ja muut yrityksen tietoturvauhat. Opinnäytetyön ovat tehneet Eetu ja Elmo Juppi vuonna 2008. Heidän opinnäytetyössään keskityttiin myös palvelunestohyökkäyksiin ja niiden torjuntaan. Työssä he selvittivät tietoturvauhkien yleisyyttä ja hyökkääjien motiiveja.

Suojelupoliisin vuosiraportissa 2012 löytyy maininta kyberuhkasta ja huoli siitä, että Valtioneuvoston julkaisema kyberstrategia ottaa huomioon viranomaisten tarvitsemat toimivaltuudet sekä viranomaisten käytännön mahdollisuudet suoriutua tehtävistään. Myös liikenneviraston tekemässä liikennejärjestelmän riskikartoituksessa 2011 on otettu huomioon kyberuhkan mahdollisuus haitata liikennejärjestelmän toimivuutta.

Paunu Pasi ja Ingalsuo Timo ovat tehneet Tampereen Yliopiston Informaatiotieteiden yksikössä raportin Kyberturvallisuus, hyökkäys ja puolustus syyskuussa 2012. Raportti on kooste Tampereen yliopistolla järjestetyllä seminaarista, jonka aiheena oli kyberturvallisuus. Raportti on kooste eri turvallisuusalojen toimijoiden, tutkimuslaitosten ja yritysten edustajien kokemuksista, heidän näkemyksistä kyberturvallisuuden ajankohtaisista asioista sekä uusimmista kehityssuuntauksista.

Useissa tutkimuksissa kyberaihetta sivutaan monellakin tapaa. Kuten Candolin Catharina, joka on kirjoittanut väitöskirjan aiheesta Securing military decision making in a network-centric environment. Hänen väitöskirjassaan aihetta käsitellään verkkokeskeisen ympäristön näkökulmasta. Candolin ja Jormakka Jorma ovat laatineet kirjan aiheesta Technical aspects of network centric warfare. Tässä heidän yhdessä laatimassaan kirjassa käsitellään verkkokeskeisen sodankäynnin teknisiä ominaisuuksia.

Hirvelä Arton diplomityö yleisesikuntaupseerinkurssilla 52, Aivomyrsky ja informaatiotulva – informaatiosodankäynnin vaikutus informaatioympäristöön käsittelee länsimaisen yhteiskunnan tilaa ja sodankäynnin muuttunutta luonnetta. Tutkimuksessaan hänkin sivuaa kyberuhkan olemassaoloa, miettimällä yhteiskunnan toimintojen muuttumista verkostokeskeisemmäksi.

Visuri Pekka on tehnyt väitöskirjan aiheesta Totaalisesta sodasta kriisinhallintaan, puolustusperiaatteiden kehitys läntisessä Keski-Euroopassa ja Suomessa vuosina 1945–1985. Ruhala Kalevi on työstänyt oman väitöskirjansa aiheesta Turvallisuuspolitiikka, Ulkopolitiikan ja strategian peruslinjat ydinaseiden aikakaudella. Heidän väitöskirjansa kuvaavat epäsuorasti uhkakuvien merkitystä valtion politiikassa.

Nokkala Arto on tehnyt väitöstutkimuksen Turvallisuuden laajeneminen ja uhkakuvien muutos, joka sisältyy hänen lisensiaattitutkimukseen. Tutkimuksessaan hän tarkastelee uhkakuvien muodostumista ja käyttöä Suomen turvallisuuspolitiikassa vuosien 1978–1994 välisellä ajanjaksolla. Hänen työnsä ei sinällään liity kyberuhkaan, mutta työssä kuitenkin käsitellään uhkakuvia ja niiden muodostumista, joka on kuitenkin samankaltaista kuin kyberuhkankin muodostamisessa.
Maanpuolustuskorkeakoulussa on tehty useita eritasoisia upseerien opinnäytetöitä, jotka kohdistuvat Suomen uhkakuviin. Muutamia esimerkkeinä niistä voisi mainita Kosonen Petri, joka on tehnyt diplomityönsä yleisesikuntaupseerikurssilla aiheesta: Suomen ja Ruotsin virallisten uhkakuvien muutoksiin vaikuttaneita tekijöitä. Ikonen Tommi on puolestaan tehnyt esiupseerikurssintutkielmansa aiheesta: Epäsymmetrinen sodankäynti ja sotilaallinen kriisinhallinta.

1.4 Tutkimusmenetelmät

Tutkimuksen teoreettisena viitekehyksenä toimii Castellsin ja Himasen luoma tietoyhteiskuntamalli. Heidän mukaansa pelkästään hyvinvointivaltio ei vielä luo tietoyhteiskuntaa. Suomen menestys tietoyhteiskuntana johtuu tehokkaasta yliopistolaitoksesta, joka on suuressa vuorovaikutuksessa teollisuuden tutkimus- ja tuotekehitystoiminnon kanssa. Informaatioteknologian klusteri on yksi osa tietoyhteiskuntaa, kuin myös luonnollisesti hyvinvointivaltio. Tietoyhteiskuntaan kuuluu voimakas kansallinen identiteetti ja kulttuuri. Suomi on hyvä yhdistelmä tietoyhteiskuntaa ja hyvinvointivaltiota. Tässä tietoyhteiskunnan kehyksessä on hyvä tutkia suomalaisen yhteiskunnan toimintaa uusia uhkia eli tässä tutkimuksessa vain kyberuhkaa vastaan. Tietoyhteiskuntamallin keskuksena toimii valtion, yritysmaailman ja yhteiskunnan muodostama troikka. Tämä kolminaisuus muodostaa keskeisen tekijän myös toiminnassa uusia uhkia vastaan (Castells, Himanen 2001, 149-160).

Tutkimus suunnataan kohti tulevaa, sellaista kohti mitä ei vielä ole. Tästä syystä lopputulos ei ole sama kuin lähtökohtatilanne. Tutkimustyö, jossa alussa tiedetään mitä lopussa tulee olemaan, ei ole tieteellistä vaan hallinnollista (Varto 2005, 22). Tätä tutkimusta aloittaessa on olemassa tiettyjä ennakkokäsityksiä, miten yhteiskunta toimii uusia uhkia vastaan. Tutkimuksen tarkoitus on selvittää tuntematon tulevaisuus sekä tutkia millainen keinovalikoima yhteiskunnalla on käytössään suojautumisessa ja millaiselta uhkalta sen ylipäätään tulee suojautua. Tutkimuksessa pyritään löytämään kyberuhkasta tärkeimmät ydinasiat yhteiskunnan kannalta. Kyberuhka yhteiskunnassa kasvaa päivittäin. Vielä on vaikea tietää vielä millaisia vaikutuksia mahdollisilla kyberiskuilla yhteiskunnan toiminnoille aiheutetaan, jos ne toteutuvat kaikkien pahimpien skenaarioiden toteutuessa. Tutkimuksen tarkoitus on helpottaa ymmärtämistä kyberuhkasta. Se, että onko ymmärrys uusien toimintaohjeiden muodostamista vai pelkästään asian avaamista yksinkertaisempaan muotoon, ei vielä voida sanoa.

Tämä tutkimus on luonteeltaan kvalitatiivinen eli laadullinen tutkimus. Laadullisen tutkimuksen keskeisimpänä tavoitteena on ymmärtää tutkimuksen kohdetta. (Virta, Johtamisen laitoksen tutkimusohje, 28). Laadullisessa tutkimuksessa kohteena on ihminen ja ihmisen elämismaailma eli merkitysten kokonaisuus, missä ihmistä voidaan tarkastella.(Varto 2005, 28).

Lähtökohtana kvalitatiivisessa eli laadullisessa tutkimuksessa on todellisen elämän kuvaaminen. Todellisuus tiedetään tai oletetaan moninaiseksi, mutta tutkimusta tehdessä on otettava huomioon, että todellisuutta ei voi pirstoa mielivaltaisesti. Kvalitatiivisessa tutkimuksessa tutkija ei voi sanoutua irti arvolähtökohdista. Ne määräävät ja muovaavat sitä, miten pyrimme ymmärtämään tutkimiamme ilmiöitä (Hirsjärvi, Remes, & Sajavaara, 2005, 152.). Kvalitatiivisessa tutkimuksessa yleisesti todetaan, että pyrkimyksenä on pikemmin löytää tai paljastaa tosiasioita, kuin todentaa jo olemassa olevia väittämiä (Hirsjärvi ym. 2005, 152).

Kvalitatiivinen tutkimusote soveltuu parhaiten tai erityisen hyvin tutkimukseen silloin, kun kiinnostus kohdistuu tapahtumisen yksityiskohtaisiin rakenteisiin eikä niiden yleisluonnolliseen jakaantumiseen. Tutkimuksen kohteena ovat tietyissä tapahtumissa mukana olevien yksittäisten toimijoiden merkitysrakenteet tai kun halutaan tutkia luonnollisia tilanteita. Tilanteet ovat sellaisia, joita ei voida järjestää kokeeksi tai niissä ei voida kontrolloida kaikkia vaikuttavia tekijöitä. Laadullinen tutkimusote soveltuu silloin, kun halutaan saada tietoa tiettyihin tapauksiin liittyvistä syy-seuraussuhteista, joita ei voida tutkia kokeen avulla (Hirsjärvi ym. 2005, 152).

Tämä tutkimus on selkeästi luonteeltaan laadullinen työ. Tutkimuksessa on tarkoitus tutkia syvällisesti yhteiskunnan varautumista kyberuhkaan ja sen ilmenemismuotoihin. Tutkimuksessa selvitetään mistä kyberuhka muodostuu, kenen taholta se on uhka ja mille tahoille se koetaan uhkaksi. Puhuttaessa kyberista, on vaikea puhua siitä muuten kuin yleisellä tasolla. Kyber sana pitää sisällään paljon informaatiota, joka voidaan tulkita monisäikeisesti. Tämän tutkimuksen tarkoituksena on avata kyberuhka yhteiskunnalle ja määritellä selkeästi sen ilmenemismuodot.

Kvalitatiivisen tutkimuksen suurimpana haasteena on pidetty sisällönanalyysiä. Laadullinen tutkimus on suurimmassa määrin käsityöläisyyttä ja luovaa. Se vaatii tutkijalta suurta lukeneisuutta sekä herkkyyttä omaan aineistoonsa. Tutkijan tulee kyetä tulkitsemaan saamiaan tuloksia. Tulkinnalla on suuri merkitys tutkimuksessa, koska oivallinen tulkinta voi lisätä ihmisen ymmärrystä arjesta (Syrjäläinen, Eronen & Värri 2008, 8).
Tutkimusmenetelmällä tarkastellaan merkitysten maailmaa, joka on ihmisten välinen ja sosiaalinen. Merkitykset ilmenevät suhteina ja niistä muodostuvista merkityskokonaisuuksista. Ne puolestaan ilmenevät ihmisistä lähtöisin olevina ja ihmisiin päätyvinä tapahtumina. Tutkimusmenetelmällä haetaan ihmisen omia kuvauksia koetusta todellisuudesta. Kuvausten oletetaan sisältävän niitä asioita, joita ihminen pitää itselleen elämässään merkityksellisenä ja tärkeinä. Tutkimusme-

netelmällä on mahdollista tavoittaa myös merkityksellisesti koettuja tapahtumaketjuja, oman elämän kulkua tai pidemmälle jaksolle sijoittuvaa asiaa. (Vilkka, 2005, 97).

Tässä tutkimuksessa avataan kyberasioita yksinkertaisempaan muotoon ja tutkitaan kyberin vaikutusta yhteiskunnan kannalta. Yhteiskunnalliset vaikutukset heijastuvat yksittäiseen ihmiseen ja näitä vaikutuksia tässä tutkimuksessa pyritään nostamaan esille.
Laadulliseen tutkimusmenetelmään liittyy aina kysymys: mitä merkityksiä tutkitaan? Tämä edellyttää tutkijalta täsmentämistä, tutkitaanko kokemuksiin vai käsityksiin liittyviä merkityksiä. Käsityksen ja kokemuksen välillä ei välttämättä aina ole yhteyttä. On tiedostettava, että kokemus on aina omakohtainen ja käsitykset tulevat pikemmin yhteisön perinteellisyydestä sekä tyypillisistä tavoista ajatella yhteisössä (Vilkka, 2005, 97).

Erityispiirteenä tälle tutkimusmenetelmälle on, että voidaan todeta tämän avulla tehtävän tutkimuksen tavoitteesta, ettei sen tarkoitus ole totuuden löytyminen tutkittavasta asiasta. Tavoitteena on tutkimuksen aikana muodostuneiden tulkintojen avulla näyttää jotakin mikä on välittömän havainnoinnin tavoittamattomissa (Vilkka, 2005, 98).

Alasuutari on todennut, että tarvitaan selkä tutkimusmetodi, jotta aineistoissa olevat havainnot voidaan erottaa tutkimuksen tuloksista (Alasuutari, 2001, 82.). Laadulliseen tutkimukseen liittyy, että sille on luonteenomaista käännellä ja katsella ilmiötä monelta kantilta sekä problematisoida jokaista itsestään selvää näkökulmaa. Kuinka siis voi tutkimuksen alkuvaiheessa lyödä lukkoon jonkin teoreettisen viitekehyksen, tuottaa metodin avulla tietynlaisia havaintoja ja tarkastella niitä johtolankoina. Laadulliselle tutkimukselle on tästä syystä luonteenomaista kerätä aineistoa, joka mahdollistaa monenlaiset tarkastelut mahdollisiksi. Näkökulmaa, linssiä ja polttoväliä voidaan mahdollisimman vapaasti vaihtaa (Alasuutari, 2001, 84).

Lähtökohtaisesti tutkimuksen taustalla on konstruktivistinen oletus tieteenfilosofiana. Filosofisella tasolla tämä antaa tutkijalle mahdollisuuden kunnon kritiikkiin. Kun, tutkimusprosessi etenee alkaa tietoa tutkittavasta asiasta muodostua. Konstruktivistille todellisuus on suhteellista todellisuutta eri henkilöiden kesken. Tutkija ja tutkittava ovat toisiinsa interaktiivisessa yhteydessä. Tutkimuksen löydökset ovat tutkijan tulkintoja tutkittavasta (Metsämuuronen 2006, 86).

Tutkimusta käsitellään teoriaohjaavan sisällönanalyysin avulla. Jouni Tuomi ja Anneli Sarajärvi ovat kuvanneet, että sisällönanalyysiksi voidaan nimittää kaikkea tutkimusaineiston tiivistämistä

ja luokittelua eri kategorioihin. Kaikissa laadullisissa tutkimuksissa voidaan käyttää perusanalyysimenetelmänä sisällönanalyysia. Sisällönanalyysi on nykypäivänä laajasti käytetty tutkimusmenetelmä juuri laadullisten aineistojen tutkimuksessa. Sisällönanalyysi ei ole kovin tarkkaan rajattu menetelmä. Tämän vuoksi se antaa tutkijalle vapauden työskennellä ilman tarkkaan säädettyjä rajoja. Sitä voidaan soveltaa yksittäisenä tutkimusmenetelmänä kuin myös teoreettisena viitekehyksenä. Tästä syystä sitä siis on helppo käyttää laadullisissa tutkimuksissa (Tuomi, Sarajärvi 2003, 93).

Tutkimusmenetelmänä sisällönanalyysia on runsaasti käytetty. Sisällönanalyysi on menetelmä, jota voidaan soveltaa sekä määrällisissä että laadullisissa tutkimuksissa. Sisällönanalyysissä aineistoa tarkastellaan eritellen. Aineistosta etsitään eriäväisyyksiä ja yhtäläisyyksiä tiivistäen tekstiä. Se on diskurssianalyysin tavoin tekstianalyysia. Tarkastelun kohteena on jo valmiita tekstimuotoisia aineistoja tai sellaisiksi muutettuja aineistoja. Sisällönanalyysin avulla aineistosta pyritään muodostamaan tiivistetty kuvaus tutkittavasta ilmiöstä ja kytkemään se laajempaan kontekstiin sekä muihin tutkimustuloksiin. Sisällönanalyysin yhteydessä voidaan puhua myös sisällön erittelystä. Sisällön erittelyllä tarkoitetaan kvantitatiivista dokumenttien analyysia. Sisällön erittelyssä kuvataan määrällisesti tekstin tai dokumentin sisältöä. Sisällönanalyysillä tarkoitetaan taas tekstin sanallista sisällön kuvailua. Se voidaan tehdä aineistolähtöisesti, teoriaohjaavasti tai teorialähtöisesti. Sisällönanalyysissä aineistoa pilkotaan osiin, aineisto käsitteellistetään ja järjestetään uudenlaiseksi kokonaisuudeksi (Saaranen-Kauppinen & Puusniekka 2006).

Sisällönanalyysissä Syrjäläisen mukaan sitä kuvataan lähes samoilla termeillä kuin Grounded theory-metodologiassa. Analyysi voidaan jakaa useisiin vaiheisiin. Ensimmäinen vaihe on tutkijan herkistyminen. Se edellyttää aineiston perinpohjaista tuntemusta sekä keskeisten käsitteiden haltuunottoa teoreettisen kirjallisuuden avulla. Toisessa vaiheessa tutkija sisäistää hankkimansa aineiston ja teoretisoi eli suorittaa ajattelutyön. Ajattelutyön jälkeen tai sen aikana tehdään karkea luokittelu. Tutkimustehtävä täsmentyy ja käsitteitä täsmennetään. Luokittelun jälkeen todetaan ilmiöiden esiintymistiheys, poikkeusten toteaminen ja suoritetaan uusi luokittelu. Ristiinvalidoinnilla tehdään saatujen luokkien puoltaminen tai horjuttaminen aineiston avulla. Lopulta tutkija on valmis tekemään johtopäätökset ja tulkinnat, jonka perustella saatu tulos siirretään laajempaan tarkastelukehikkoon (Metsämuuronen 2006, 124).

Tämän tutkimuksen aineisto käsitellään teoriaohjaavan sisällönanalyysin avulla. Teoriaohjaava sisällönanalyysi aloitetaan tutustumalla aineistoon. Tässä tutkimuksessa käytetään aineiston ke-

ruumenetelmänä dokumentteja eli kirjallisuuslähteitä. Primaarilähteitä tutkimukseen on hankittu keräämällä aiheeseen liittyviä dokumentteja eli kirjallisuutta ja aikaisempia tutkimuksia, joiden tutkimuskohde on ollut lähellä tämän tutkimuksen aihetta. Tutkimukseen on käytetty sekundaarilähteinä internet-lähteitä, lehtiartikkeleita ja raportteja mitä eri viranomaistahot sekä oppilaitokset ovat tuottaneet kyberuhkasta.

Keskeisen aineiston kerääminen ja käsitteleminen oli haastavaa, koska suomenkielistä kirjallisuutta kyberasioista ei ole julkaistu vielä kattavasti. Internetin kautta on saatavilla runsaasti erilaisia keskusteluja ja mielipiteitä kyberista. Aineiston moninaisuudesta johtuen päädyttiin tekemään tutkimus teoriaohjaavan sisällönanalyysin avulla, koska se mahdollistaa tutkijalle väljän analyysirungon. Tutkimuksessa käsitellään kyberin mahdollistamia uhkia sekä analysoidaan vastaako Suomen kansallinen kyberstrategia näihin uusimpiin uhkiin. Viitekehyksenä tutkimuksessa on tietoyhteiskunta. Tietoyhteiskunta käyttää apunaan kansallisen kyberturvallisuusstrategian ja yhteiskunnan elintärkeiden toimintojen turvaamisen strategian antamia ohjeistuksia sekä vaatimuksia. Tätä runkoa käyttämällä kyettiin jättämään tutkimuksen ulkopuolella asiat, jotka olivat tutkimukselle vähemmän merkityksettömiä.

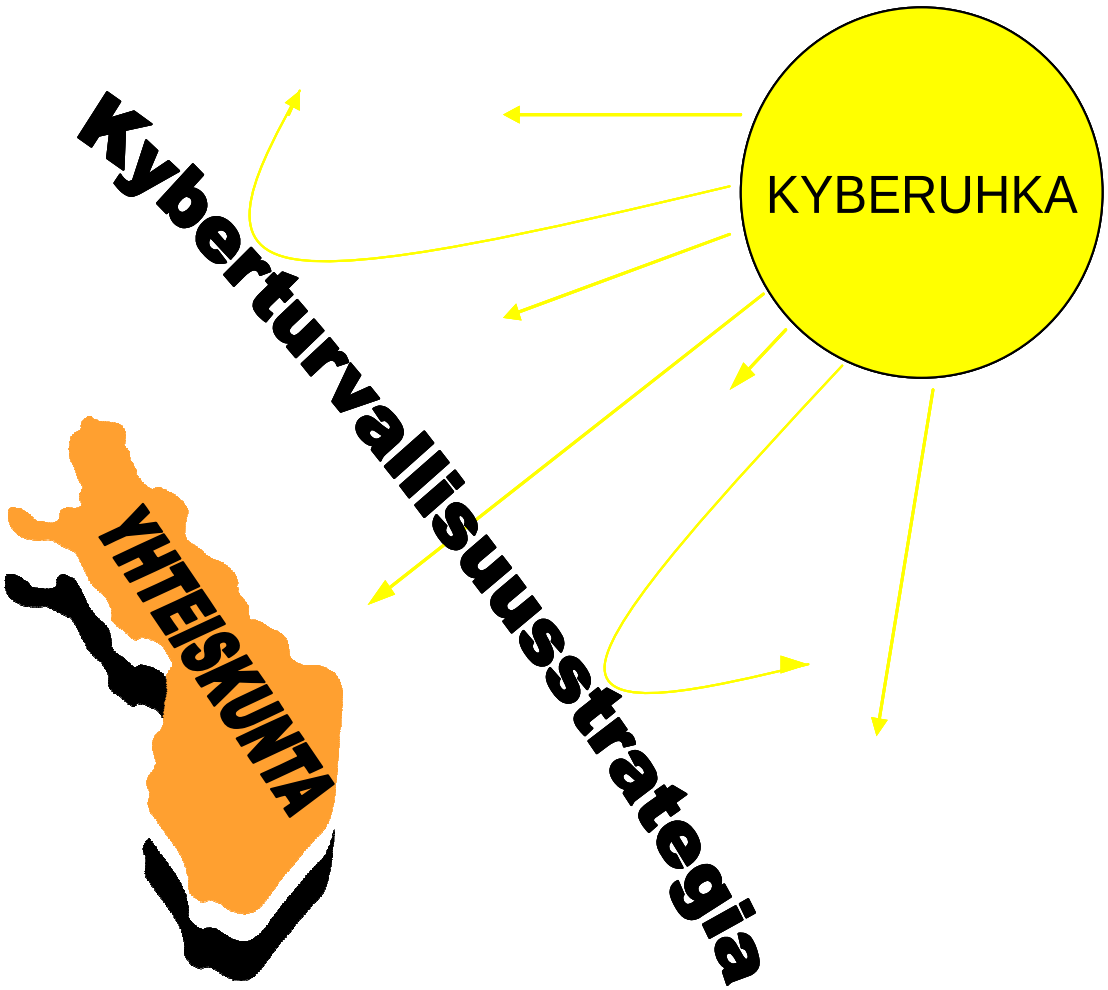
Aineistosta valitaan analyysiyksiköt, vaikkakin aikaisempi tieto ohjaa analyysin tekoa. Aineisto pyritään pelkistämään ja lopuksi pelkistetyt ilmaukset ryhmitellään sisällön mukaan omiin luokkiinsa. Teoreettiset käsitteet liitetään osaksi analyysia loppuvaiheessa, jolloin teorian merkitys on korostunut (Tuomi & Sarajärvi 2003, 98 - 99). Analyysi suoritetaan täysin aineiston ehdolla, abstrahointivaiheessa kaikki teoreettiset käsitteet liitetään empiiriseen aineistoon (Tuomi & Sarajärvi 2003, 110 - 117).

Abstrahointi tarkoittaa tutkimuksessa koostetta, jossa yhdistyy analyysi ja synteesi. Analyysissa kerätty tieto käsitteellistetään eri osiksi ja synteesin avulla saadut osat kootaan uudelleen tieteellisiksi johtopäätöksiksi. Saadut johtopäätökset eivät enää edusta tutkittavia tapauksia, vaan johtopäätökset siirtyvät yleisemmälle käsitteellisemmälle ja teoreettiselle tasolle (Metsämuuronen 2006, 122).

Kerätystä aineistosta poimittiin kyberuhkaan liittyvät keskeisimmät asiasisällöt jotka olivat tämän tutkimuksen kannalta merkittäviä. Rajaaminen ei ollut kuitenkaan yksiselitteistä, koska kyber muodostuu kokonaisuudessaan niin pienistä elementeistä, että tietoa niistä oli enemmän kuin tarpeeksi. Asiat, mitkä jouduttiin jättämään tämän tutkimuksen ulkopuolelle, ovat kuitenkin olleet taustalla ja auttaneet varsinaisen analyysin laatimisessa. Keskeisimmät asiasisällöt käytiin läpi avaten ja kertoen taustoista sen mitä lukija tarvitsee ymmärtääkseen kokonaisuuden paremmin.

Kokonaisuudessaan teoriaohjaavassa analyysissä on kyse abduktiivisesta päättelystä (Tuomi & Sarajärvi 2009, 97). Abduktiivinen päättely on yksinkertaisimmillaan loogista päättelyä, siitä on puhuttu myös arvaamisesta. Teoria voidaan muodostaa silloin, kun saatuihin havaintoihin saadaan liitettyä johtoajatus tai johtolanka. Jos tutkimuksessa halutaan painottaa päättelyä, niin silloin tutkimuksen yhteydessä voidaan puhua induktiivisesta analyysista (Tuomi, Sarajärvi 2003, 97–98).

Tässä tutkimuksessa kuvataan lukijalle kyberin kautta ilmeneviä uhkia sekä esitetään niille ratkaisumalleja. Kuvassa 1 on tutkimuksen viitekehys visuaalisesti esitettynä. Tutkimus pitää sisällään paljon samankaltaisuuksia. Tietoyhteiskunnan rajauksella ja erilaisten strategioiden avulla sekä dokumenteista saaduilla tiedoilla pyrittiin tekemään yksinkertaiset päättelyt, jotka yhdistettiin kyberstrategian keskeisimpiin osa-alueisiin.



Kuva1. Tutkimuksen viitekehys

1.5 Käsitteiden määrittely

Ilman riittävää perusymmärrystä keskeisimmistä määritelmistä, on vaikea ymmärtää tutkimuksen sisältöä. Seuraavaksi tutkimuksessa esitellään lyhyesti muutamia tutkimuksen kannalta keskeisimpiä määritelmiä. Epäsymmetrisiä uhkia ja kyberuhkia käsitellään laajemmin myöhemmin tässä tutkimuksessa.

"*Yhteiskunta* on jäsentensä keskinäisiin suhteisiin perustuva järjestetty kokonaisuus, jossa kaikki ihmisten elämälle tarpeellinen yhteistoiminta tapahtuu." (Koukkunen, 1990,672).

Yhteiskunnan toimimisen kannalta on määritelty sille elintärkeät toiminnot. Yhteiskunnalle elintärkeät toiminnot ovat perusedellytys yhteiskunnan olemassaololle. Häiriöt niiden toiminnoissa vaikuttavat keskeisesti kansalaisten arkeen ja elämään.

Yhteiskunnan elintärkeitä toimintoja ovat:

– valtion johtaminen
– kansainvälinen toiminta
– valtakunnan sotilaallinen puolustaminen
– sisäisen turvallisuuden ylläpitäminen
– talouden ja infrastruktuurin toimivuus
– väestön toimeentuloturva ja toimintakyky sekä
– henkinen kriisinkestävyys

(Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, 2006,13)

” Terrorismi on poliittisesti motivoitunutta väkivallan käyttämistä tai sillä uhkaamista, jonka tarkoituksena on aiheuttaa vakavaa pelkoa väestön keskuudessa, pakottaa oikeudettomasti jonkin valtion hallitus, viranomainen tai kansainvälinen järjestö tekemään, sietämään tai tekemättä jättämään jotakin, kumota oikeudettomasti jonkin valtion valtiosääntö, muuttaa sitä tai horjuttaa vakavasti valtion oikeusjärjestystä, tai aiheuttaa erityisen suurta vahinkoa valtion tai kansainvälisen järjestön taloudelle tai muille perusrakenteille.” (Yhteiskunnan turvallisuusstrategia, 16.12.2010, 2011,92)

Kyberavaruus käsite on vakiintunut alan termistöön, mutta kuitenkaan Suomessa sitä ei juuri käytetä. Termi kuitenkin tulee esille lukuisissa dokumenteissa missä käsitellään kyberia. Kyberavaruus on kaikkien tietokoneiden välinen verkosto maailmassa ja kaikkialla missä tietokoneet ovat yhdistettyinä sekä valvomassa. Kyberavaruus ei ole pelkästään internet. Internet on avoin verkosto verkoston sisällä. Kyberavaruus sisältää internetin ja paljon muita verkostoja minkä tietokoneilla ei oleteta olevan yhteyksiä internetiin. Yksityiset verkostot muistuttavat internetiä, mutta kuitenkaan ne eivät ole sitä, vaan ovat ainakin teoreettisesti erillään siitä. Osa kyberavaruutta on kaupallinen verkosto, joka kautta kaikkea rahaliikennettä pyöritetään. Kyberavaruudessa on verkostoja, jotka ovat erilaisten koneiden ja järjestelmien välillä. Tämänkaltaisissa verkostoissa toimivat muun muassa erilaiset viemäriverkoston ohjaimet, hissit sekä muut tämän kaltaiset laitteet (Clarke & Knake, 2010, 69–70).

”Kyberuhka tarkoittaa mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnon. Kybertoimintaympäristöön kohdistuvat uhkat ovat tietoturvauhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan.” (Suomen kyberturvallisuusstrategia, 2013, 13).

”*Kyberturvallisuudella* tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Tarkennus 1 - Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle.

Tarkennus 2 - Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä (”yhteisöllinen tietoturva”). Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia.

Tarkennus 3 - Kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle.” (Suomen kyberturvallisuusstrategia, 2013, 13).

2. KYBER – YHTEISKUNNAN UUSI UHKA

Tiedonvälityksen tehostuminen on tehnyt yhteiskunnasta entistä tietoisemman erilaisista uhkista. Uhkavalikoima on laajentunut ja lisännyt yhteiskunnan haavoittuvaisuutta lisääntyneen informaatioteknologian myötä. Virushyökkäykset tai tietoverkkorikollisuus eivät olisi mahdollisia ilman teknisen kehityksen ja verkostoitumisen lisääntymistä. Uhkakuvien lisääntymisestä on seurannut laajempi varautuminen turvallisuuden ylläpitämiseen. Turvallisuuden kiistanalaisuus ja turvattomuuden ilmapiiri on lisääntynyt (Limnéll, 2009, 7).

Perinteisesti uhkakuvat ovat olleet keinoiltaan sotilaallisia ja aiheuttajiltaan valtiollisia. Nykyään varaudutaan laajempiin uhkakuviin ja painopiste on muissa kuin sotilaallisissa uhkissa. Turvallisuuspolitiikka on lähtökohdiltaan kokonaisvaltaista (Turvallisuuspoliittinen seurantaryhmä, 2008, 33).

Uhka on ollut osa politiikkaa niin kauan kuin ihminen on muodostanut yhteisöjä. Tieteellisessä ja poliittisessa keskusteluissa uhkien torjuntaa kutsutaan turvallisuudeksi (Vuori 2005, 2). Nykyään yhteisöjen muodostumista tapahtuu sähköisten palveluiden kautta. Yhteisöt ja palvelut ovat osa sähköistä tietoliikennettä. Ajallemme on tyypillistä niin sanottu turvallistaminen, joka on uhkakuvamuutoksista puhuttaessa huomionarvoisa kehityssuunta. Useat ilmiöt ja asiat nähdään sekä yhteiskunnalliset ongelmat mielletään turvallisuuskysymyksiksi. Tämä ajattelumalli muuttaa poliittista suhtautumista sekä keinovalikoiman muutosta joita käytetään syntyneiden ongelmien ratkaisemiseen. Turvallisuus on osittain niin sanottu muoti-ilmiö. Se liitetään ilmiönä ja käsitteenä helposti uusiin asioihin. Seurauksena tästä on, että tätä uutta turvallisuuden tarvetta tuottamaan yhteiskunnalle sekä jonkin tahon pitää keskittyä hallinnoimaan sitä (Puolustusministeriö, 2012, 6).

Useimmat yhteiskunnan palvelut ja toiminnot ovat kiinteästi sidoksissa tietoliikenteen kautta sähköisiin palveluihin. Suurin osa yhteiskunnan kriittisistä palveluista perustuu sähköiseen tiedonsiirtoon ja tietovarantojen käyttöön. Näitä yhteiskunnan palveluita ohjataan tietoteknisesti tai ne ovat kokonaan sähköisiä palveluja. Palvelut, järjestelmät ja niitä yhdistävät tiedonsiirtoverkot sulautuvat sekä verkostoituvat laajoiksi globaaleiksi kokonaisuuksiksi. Globaalissa järjestelmässä toimintahäiriöt voivat laajeta yksittäisistä palveluista laajemmiksi, koskettaen järjestelmäkokonaisuuksia. Teknologia on kehittynyt ja kehittyy huimaa vauhtia. Mobiiliratkaisut, sekä internet

korostuvat viestinnän muotoina. Tämä sähköinen infrastruktuuri muodostaa haavoittuvan ja vaikeasti hallittavan kokonaisuuden. Uhka on erittäin merkittävä ja sen merkittävyyttä lisää se, että sähköenergian varassa toimivia tieto- ja viestintäjärjestelmiä käytetään yhteiskunnan johtamiseen sekä väestön varoittamiseen niin häiriötilanteissa kuin poikkeusoloissa. Voidaan sanoa, että uhka kohdistuu kaikkia kohtaan jotka käyttävät sähköisiä palveluita. (Yhteiskunnan turvallisuusstrategia 2011, 66).

Ymmärtääkseen tutkittavaa aihetta eli kyberuhkaa, on ymmärrettävä mitä sana kyber tarkoittaa. Kyber – sana juontaa juurensa kybernetiikasta, jonka Wiener on määritellyt vuonna 1948 omaksi tieteekseen. Kybernetiikalla hän tarkoittaa tiedettä, missä elollisen olennon ja koneen välistä kommunikaatiota, viestintää toteutetaan (Ashby 1957, 1).

Vuosien 1985 – 1990 tienoilla ryhdyttiin käyttämään ilmausta ”cyberspace.” Termin otti käyttöönsä ensimmäisenä William Gibson. Hän käytti sanaa vuonna 1984 julkaistussa tieteiskirjassaan Neuromancer. William Gibson määritteli sanan cyberspace seuraavalla tavalla:
"Cyberspace: A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding. . ." (Gibson 1984, 128).

Vapaasti suomennettuna Gibsonin määritelmä on seuraavanlainen:
” Konsensuaalinen, yhteisymmärryksellinen aistiharha on jotain sellaista, jonka päivittäin kokevat miljardit legitiimit toimijat eri puolilla maita ja kansakuntia sekä (esimerkiksi) lapset, joille opetetaan matemaattisia malleja ja käsitteitä..., ja jota tekee/aiheuttaa sellaisen tiedon graafinen esittäminen, joka on alun perin tuotettu pankkien tietokoneilla (tai pankkijärjestelmiä ylläpitävillä tietokoneilla). Käsittämättömän monimutkaista. Valon säikeet vaihtelevat muotoaan mielen tiedottomuudessa, samoin vaihtelevat tiedon lukuisat eri kokoonpanot ja muodot”.

Suomennettuna Gibsonin määritelmä on todella hankala ymmärtää, mutta kun ymmärtää kontekstin niin voi ymmärtää hänen kyberavaruuden määritelmänsä. Kyberavaruus ymmärretään olevan laaja, vastaavanlainen olomuoto kuin avaruus ympärillämme. Se pitää sisällään valtavan olemassaolon sekä tiedon laajuuden, jonka sisältöä ja kokonaisuutta on mahdoton käsittää ymmärtäen sitä täysin. Perinteinen kysymys mihin avaruus päättyy, voidaan esittää myös kyberavaruuden

kohdalla. Kyberavaruutta on vaikea rajata kunnolla. Gibsonin määritelmästä on jo aikaa, ja tänä päivänä kyberavaruus internetmaailmassa on lähestulkoon ääretön, jatkuvasti laajentuva kokonaisuus.

Kuten Gibson jo totesi, kyberavaruus sanalla ei ole tarkkaa määritelmää. Sitä käytetään yleensä kuvaamaan tietokoneiden virtuaalista maailmaa. Internetin myötä kyberavaruus kattaa globaalin tietokoneiden välisen verkoston. Esimerkiksi lähettäessä sähköpostia, puhutaan viestin lähettämisestä kyberavaruudessa (Techterms, cyberspace).

Kyberavaruus terminä on kuitenkin yleistynyt käytössä 1990-luvulla, jolloin kyberavaruus nähtiin täysin erilaisena kuin normaali fyysinen maailma. Kyberavaruus on kuitenkin oma fyysinen toimintaympäristö, koska on se fyysisten järjestelmien luoma yhteyksien verkosto. Tätä järjestelmää ohjaavat erilaiset tietokonepohjaiset softat ja yhteysprotokollat. Yhdysvalloissa kyberavaruuden merkitystä operatiivisella tasolla on korostettu, 9/11 iskujen jälkeen kyberavaruudesta onkin tullut tärkeä strateginen tekijä ja sitä on kutsutta uusien operaatioiden näyttämöksi (Kramer, Starr, Wentz 2009, 254).

Yhdysvalloissa tapahtuneen 9/11 World Trade Centerin tuhoisien iskujen jälkeen terrorismi militarisoitiin. Terrorismista tuli sellainen uhka, mitä vastaan on sallittua taistella sotilaallisin keinoin. Tämä niin sanottu henkinen laillistaminen vastata terrorismiin on muuttanut suhtautumista terroristien harjoittamaan toimintaan kyberavaruudessa (Puolustusministeriö, 2012, 11).
Kyberavaruuden toimintavälineinä tietokoneet ovat keskeinen työkalu. Tietokoneen keksimisen jälkeen teknologia kehittyi nopeasti. Toiminta siirtyi ja siirtyy yhä enenemässä määrin tietoverkkojen sekä niiden varaan rakennettujen komponenttien päälle. Aikaisessa vaiheessa osattiin jo ennustaan, että tällaisessa uudessa kehittyvässä virtuaalisessa toimintaympäristössä olisi sotilaallinen ulottuvuus. Alkuun tätä pidettiin täysin nörttien puuhasteluna, mutta melko nopeasti alkoi harrastepohjaisesta hakkeroinnista muuntautua tavoitteellisen rikollisuuden ja valtiollisen toiminnan suuntaus (Candolin, 2012, 5).

Tietokoneet mielletään verkkojen tyypillisiksi osiksi. Verkottuneen tietokonejärjestelmän avulla voidaan yhdistää eri puolilla maailmaa hajallaan olevia informaatio, data, teksti kuva ja myös äänitiedostoja sekä luoda näistä hajallaan olevista informaatioista uusia tiedon yhdistelmiä. Tietokone mahdollistaa viitemateriaalin laajemman ja syvällisemmän tutkinnan kuin koskaan aikaisemmin perinteisen tekstiaineiston kanssa. Verkostoitumisen perusmuotona voidaan pitää sähkö-

postijärjestelmää. Yhteenliitettyjen verkkojen välillä viestit saavuttavat vastaanottajansa muutamien sekuntien kuluessa lähetyksestä. Sähköposti voi synnyttää lukuisia keskustelulinjoja, uutisryhmiä ja erilaisia elektronisia ilmoitustauluja. Näitä ilmoitustauluja on kuvattu myös antiikin foorumin vastineeksi. Sähköpostidokumenttien maailma on epävakaa ja kaoottinen, vaikeasti hallittava sekä mahdoton kartoittaa. Selkeyttä tähän kaaokseen kehittyi luomaan World Wide Web eli WWW. World Wide Web-sivut muodostat kiinteän dokumenttiavaruuden, jota on helppo tutkia (Nyiri 1997, 25). WWW-sivustot muodostavat kattavan internetverkoston.
Kyberavaruus perustuu internetiin, kuten Viron kyberstrategia toteaa (Cyber security strategy, Estonia 2008). Kyberavaruus ymmärretään maailmanlaajuiseksi, internetiin sidoksissa tai sen ympärillä pyörivään järjestelmään. Siitä on käyttänyt nimitystä The Net Yhdysvaltojen omassa Maanpuolustuskorkeakoulussa Libicki Martin.
” The Net is the converging global system which puts people and their information in close electronic contact with each other. The growth of the Net, by permitting subnational and transnational communities, alters the basis for international conflict. The Net, itself, however, presents certain exploitable vulnerabilities for societies that depend on it”(Libicki 1994, 94).

Maailmanlaajuisesta tietokoneiden välisestä järjestelmästä on tullut uusi pelikenttä tietoverkkorikollisuudelle. Tietoverkkorikollisuus on rikollista toimintaa, jossa rikoksen välineinä käytetään internetiä ja tietokoneita (Techterms, cybercrime). Tietoverkkorikollisuutta voidaan määritellä myös erilaisin tekotavoin. Niitä ovat muun muassa tietomurrot, palvelinestohyökkäykset, identiteettivarkaudet ja laittomat tietosisällöt. Laiton tietosisältö tarkoittaa yleensä tekijänoikeussuojatun materiaalin levittämistä, lapsipornoa ja vihapuheita eri kansallisuuksia tai etnisiä ryhmiä kohtaan. Tietoverkot mahdollistavat myös rikollisten toimintaa verkossa, missä he voivat pitää yhteyttä toisiin rikollisryhmittymiin, valmistella ja suunnitella näin rikoksia. He voivat hyödyntää näin verkkoa taloudellisiin ja terroristisiin tarkoituksiin (Sisäasiainministeriö, tietoverkkorikollisuus).

Tietoverkkorikollisuudessa on mahdollisuus ansaita rahaa helposti ja siinä on alhainen kiinnijäämisen riski. Lainsäädäntö tulee hieman jälkijunassa tietoverkkorikollisuuden tunnistamisessa, sillä lain puitteissa moni asia on jäänyt tunnistamatta rikokseksi, vaikka tekijä olisikin tavoitettu. Tietoverkkohyökkäyksen kohteiksi voi joutua niin yksittäinen ihminen kuin yrityskin. Terroristit ja ääriryhmittymät käyttävät kyberavaruutta taitojensa kehittämiseen. Kyberavaruutta on käytetty jo runsaasti propagandan levittämiseen, rahankeruuseen ja – pesuun, uusien henkilöiden rekrytoimiseksi sekä koulutukseen. Vielä ei ole ollut tapausta, jossa kyberavaruutta olisi käytetty saa-

maan samankaltaista tuhoa aikaan kuin normaalissa perinteisen pommin käytössä. Toiminnasta on tullut valtiollista ja asevoimat ovat tunnustaneet kyberavaruuden yhdeksi toimintaympäristöksi. Tiedustelusta on tullut arkipäivää. Niin kutsuttu haktivismi on lisääntynyt kyberavaruudessa (Candolin, 2012, 6).

Haktivismilla (hacktivism) tarkoitetaan internetissä toimivaa, tietokone ja verkkovälitteisen aktivismin eri muotoja. Haktivismi on osa kansalaisaktivismia. Se voi käyttää hakkereiden keinovalikoimaa, mutta toisaalta hakkerit voivat edistää myös omia etujaan. Haktivismilla viitataan yhteiskunnallisiin liikkeisiin, jotka ottavat käyttöönsä tietoverkkojen mahdollisuudet omatoimisesti tai hakkereiden avustamana. Haktivismissa on teknologialla vain välineellinen rooli. Hakkerit mieltävät haktivismin aktivismiksi, jossa vastustetaan teknologiaan ripustettuja asiakysymyksiä, kuten internet-sensuuria (Jyväskylän yliopisto, haktivismi).

Hakkerit eivät alkuperäiseltä tarkoitukseltaan olleet kuitenkaan rikollisia vaan ihmisiä, jotka nauttivat ohjelmoinnista ja verkottumisesta samanhenkisten ihmisten kanssa. He ovat olleet poikkeuksellisen suuressa roolissa suomalaisessa informaatioteknologian vallankumouksessa. He toivat internetin Suomeen maailman kärjessä ja edistivät sen nopeaa leviämistä (Castells, Himanen 2001, 64).

Kyber ei tietenkään ole ainoa asia, mikä uhkaa sähköisten palveluiden ja viestinten toimivuutta. Niitä uhkaavat myös luonnonilmiöt, inhimillinen toiminta tai yksinkertaisesti tekniikan pettäminen. Viime vuosina on kuitenkin yleistynyt menetelmäksi häiritä palveluita internetin kautta tehtävillä palvelunestohyökkäyksillä. Niiden tarkoitus on tilapäisesti kuormittaa verkkopalvelimet tai palveluntarjoajan toimintakapasiteetti automaattisesti muodostettavilla viesteillä. Verkon tahattomat tai tahalliset häiriöt voivat kohdistua kaikkiin sellaisiin toimijoihin, joilla on käytössään tietoliikenne ja verkkopalveluita toiminnoissaan. Uhka voi kohdistua siis kaikkiin tahoihin, joilla on käytössään sähköisiä palveluita. Hyökkäykset kohdistuvat yleensä verkko-operaattoreita tai sähköistä kauppaa harjoittavia yrityksiä vastaan, mutta kohteina ovat myös teollisuus, yhteisöt ja muut julkiset palvelut.
Järjestäytynyt rikollisuus ja terrorismi ovat havainneet tietoverkkojen haavoittuvuuden. Tietoliikenne ja sähköiset palvelut ovat yhteiskunnallisesti merkittäviä. Tästä johtuen ne ovat tärkeitä elementtejä poliittisissa ja sotilaallisissa kriiseissä. Monien valtioiden sotilaalliseen varautumiseen on liitetty valmius tietojärjestelmien häirintään, hyväksikäyttöön ja tuhoamiseen. Informaatiosodankäynnistä on tullut kiinteä osa nykyistä sotilaallista varautumista. Verkonhallinta ja kriit-

tiset varaosavarastot sijaitset useimmiten Suomen ulkopuolella. Useimmat kriittiset järjestelmät toimivat vain muutamissa palvelukeskuksissa. Esimerkiksi Suomessa maksuliikenne on riippuvainen tietoliikenteen, tietojärjestelmien toiminnasta ja sähköenergiasta (Yhteiskunnan turvallisuusstrategia 2011, 66–67).

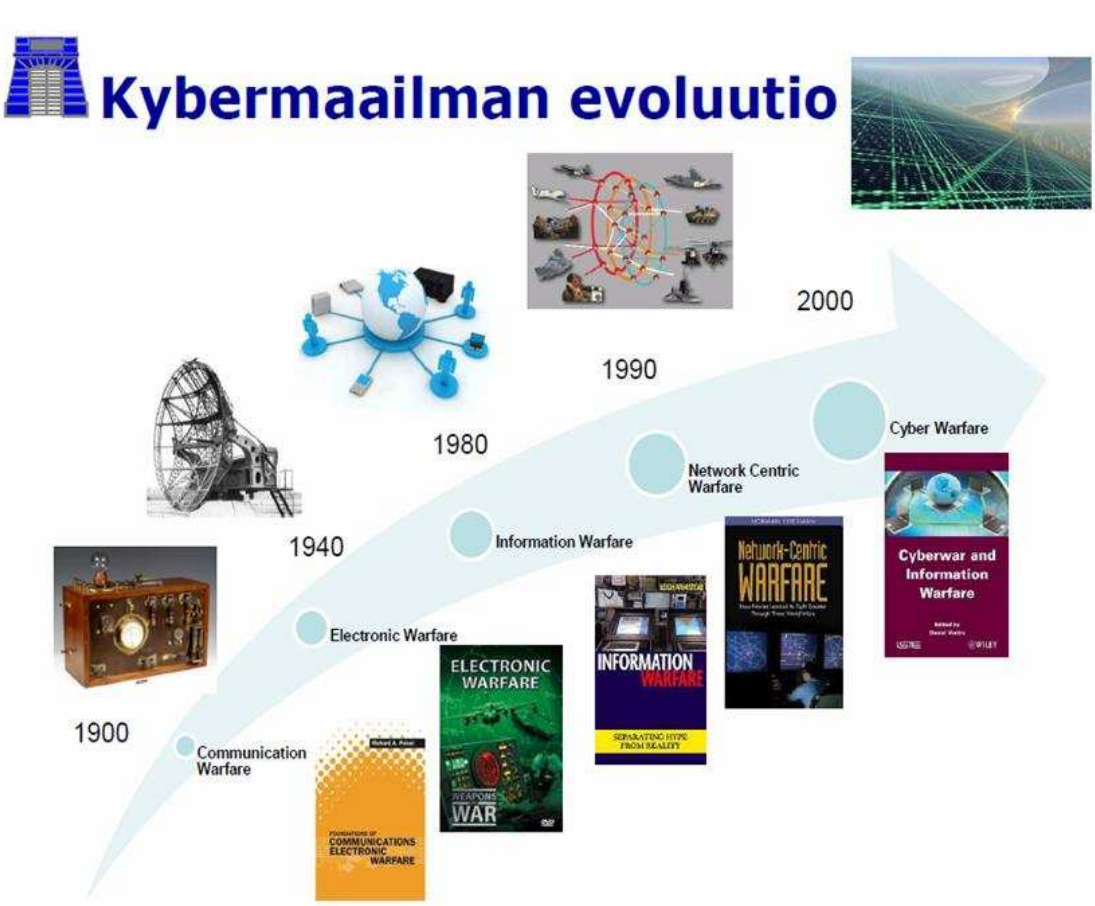
Kyberhyökkäykset voivat tuottaa suuria häiriöitä ja lamauttaa osia kriittisestä infrastruktuurista sekä yhteiskunnalle tärkeistä toiminnoista. Valtioita tai organisaatioita voidaan painostaa kyberhyökkäyksillä. Painostus voi olla poliittista, sotilaallista tai taloudellista. Monet suurvallat rinnastavat kyberhyökkäykset jo sotilaallisiksi keinoiksi ja niihin voidaan vastata kaikin mahdollisin avuin (Suomen kyberturvallisuusstrategian taustamuistio 2013, 3).

Kyberuhkan toteutuminen voi olla pidemmän aikavälin tapahtumasarja, jossa rikolliset toimivat tietynlaisen strategian avulla, joko suunnitelmallisesti tai ihan sattumanvaraisesti. Kaava on yleensä kaikissa kyberhyökkäyksissä sama, riippuen kohteesta tai tekijästä. Yleistäen voidaan todeta, että ensimmäisessä vaiheessa, suunniteltaessa kyberhyökkäystä on tiedusteltava aiottua uhria / kohdetta. Tarkkailemalla kohteen normaalia toimintaa voidaan saada hyödyllistä tietoa kuten millaisia laitteistoja ja ohjelmistoja käytetään. Millaisia viestintäkeinoja ja muotoiluja viestinnässä käytetään. Toisessa vaiheessa tunkeudutaan järjestelmään ja odotetaan mahdollisuutta häiritä tai estää tiettyjen palvelimien käyttöä. Kolmannessa vaiheessa tunnistetaan ja laajennetaan sisäisiä mahdollisuuksia päästä järjestelmän rajoitetuille sekä arvokkaammille alueille. Neljännessä vaiheessa tunkeutuja saa aikaan vahinkoa järjestelmälle niin sanotusti takavarikoimalla tai muuttamalla tietoja. Viimeisessä vaiheessa voidaan poistaa kaikki todisteet tunkeutumisesta järjestelmään ja mahdollisen varkauden, peittämällä tunkeutujan sähköisen jäljen muuttamalla tai poistamalla lokitiedostot (Janczewski & Colarik 2007, xv).

Helpoiten teollisia yhteiskuntia voidaan häiritä ja vaikeuttaa niiden toimintaa on hyökätä sähköverkoston kimppuun. Internet verkon toiminta on riippuvainen sähkönsaannista. Sähkönjakelun päättyminen katkaisee kaikkien järjestelmien toiminnan mitkä ovat toimineet verkossa. Mahdollinen verkon kaatuminen on vaikutuksiltaan pelottava. Niin sanottu sodankäynti hakkereiden ja turva-alan välillä on suhteellisen jatkuvaa toimintaa. Tilanne kärjistyy ajoittain puolin ja toisin. Turvajärjestelmät paranevat, mutta aina ilmenee uusia mahdollisuuksia kiusantekoon ja siten hakkerit saavat tasoituksia. Onneksi tällaisilla hyökkäyksillä on vähäisiä vaikutuksia. Tietokonevirukset ja niiden leviäminen on yleinen sekä yksinkertainen tapa haitata verkon toimivuutta (Libicki 1994, 109–111).

Kyberuhkat voidaan jakaa eri tasoihin nousevassa järjestyksessä. Alimmalla tasolla on kybervandalismi ja hakkerointi. Ne ovat tasoista matalimmalla ja niin sanotusti normaalikäyttäjän tekemiä toimenpiteitä. Toinen taso on järjestäytynyt rikollisuus, kolmas taso on kybervakoilu, neljäs taso on kyberterrorismi, viides taso taktinen kybersota ja kuudes, viimeinen taso on strateginen kybersota (Benson 2011, 12).

Kyberuhkat ovat kokeneet siis muutoksen ja samoin on käynyt myös kybermaailmalle. Kybermaailman muutosta kuvaa hyvin kuva 2, josta nähdään miten kybermaailman evoluutio on nopeasti muuttunut ja kehittynyt uhkaavampaan suuntaan.



Kuva 2: Kybermaailman evoluutio, Turvallisuusforum

2.1 Toiminta kyberissä

Oli kyse sitten harrastelijoista tai ammattimaisista rikollista niin heidän keinonsa toimia internet-verkossa ovat lähestulkoon samankaltaisia. Osa hyökkääjistä tekee tietoturvarikoksia ainoastaan näyttämisen halusta ja osalla taas motiivina on ansaita rahaa tai tehdä jokin asia tunnetuksi. Niin sanottujen hyökkääjien käyttämiä keinoja ovat haittaohjelmat. Haittaohjelmista tunnetuimpia ovat virukset, madot ja vakoiluohjelmat. Näitä saadaan levitettyä helpoiten sähköpostin välityksellä, ladattaessa internetistä tiedostoja tai vertaisverkon kautta. Virukset leviävät myös siirrettävien tallennusvälineiden ja levyjen kautta. Haittaohjelmista voi tulla monenlaisia harmeja tietokoneen käyttäjälle. Tietokoneen käyttö voi hidastua, verkkosurffailu ja sähköpostin käyttö hankaloitua. Haittaohjelmat vaikuttavat myös ohjelmistojen toimintaan. Tietokoneelta saattaa myös kadota tiedostoja. Sähköpostimadoista tulee ongelma tietokoneelle. Ne voivat muuttaa tietokoneen roskapostin välityspisteeksi ja tämä kaikki voi tapahtua ilman tietokoneen käyttäjän huomaamista. Verkkomadot ovat ongelmallisia, kuten Sasser ja Blaster. Ne hakeutuvat verkon välityksellä tietokoneille, missä ei ole viimeisimpiä päivityksiä. Näiden perinteisten virusten ja matojen lisäksi on olemassa haittaohjelmatyyppejä, joista yleisimmät ovat troijalaiset ja botit. Muita samankaltaisia ohjelmia ovat takaportit, vakoiluohjelmat, mainosohjelmat ja rootkitit (Viestintävirasto, Tietoturvaopas 2008).

Tietokoneohjelmaa, mikä on saanut tartunnan, kutsutaan Troijan hevoseksi. Se on ohjelma, joka suorittaa vain näennäisesti jotain hyödyllistä tai välttämätöntä, mutta samanaikaisesti suorittaa viruskoodin. Virus ei välttämättä ole kenenkään erikseen luoma, vaan on olemassa mahdollisuus, että se on virheellinen ohjelma, joka käyttäytyy toisin kuin sen oli alun perin tarkoitus (Hedemalm 2000, 223–224).

Palvelunestohyökkäykset ovat yleistyneet huomattavasti niiden alkuajoista. Ensimmäisenä merkittävänä palvelunestohyökkäyksenä voidaan pitää vuonna 1988 Morris-madon avulla tehtyä hyökkäystä. Siitä seuraavien kuuden vuoden aikana hyökkäyksiä kirjattiin CERT-organisaation tilastoihin 143. Vertailun vuoksi voidaan mainita, että joulukuussa 2010 itsenäisyyspäivän aikana, havaittiin 1626 eri hyökkäystä. Tämä siis tapahtui pelkästään yhden vuorokauden aikana. Palvelunestohyökkäykset voidaan jakaa kolmeen eri luokkaan. Luokkia ovat verkkokapasiteetin kulutus, resurssien kyllästäminen ja järjestelmien sekä sovellusten kaataminen (Björkman 2010, 1 - 2).

Ernst & Young turvallisuuskeskuksen teknologiajohtaja Say Chen on luokitellut palvelunesto-hyökkääjät viiteen eri luokkaan:

– Hauskuuttajat
– Aktivistit
– Terroristit
– Kilpailevat yritykset
– Armeija

(Chen 2007, 6)

2000-luvulla on havaittu useita erilaisia kyberhyökkäyksiä, joista muutamat ovat nousseet laajuutensa vuoksi esille. Vuonna 2007 Viro joutui laajojen palvelunestohyökkäysten kohteeksi niin kutsutun patsaskiistan aikana. Patsaskiistassa kyse oli Tallinnassa sijaitsevan pronssisoturin siirrosta. Siirto aiheutti erimielisyyksiä virolaisten ja virossa asuvien venäläisten välille. Kiista sai suuret mittakaavat ja laajeni lopulta Viron sekä Venäjän väliseksi miekkojen kalisteluksi.

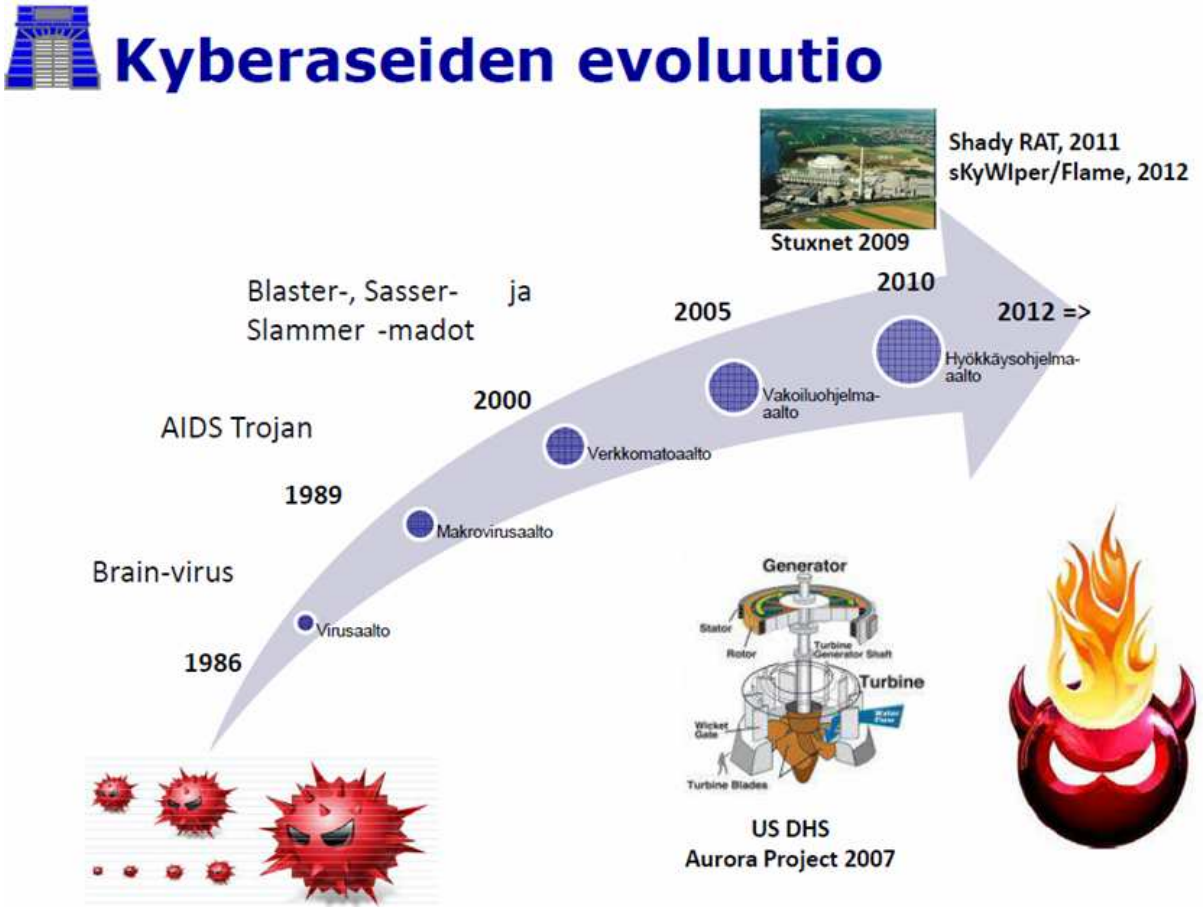
Palvelunestohyökkäyksiä kohdistettiin Viroon kaikkiaan 197:n eri valtion verkkoavaruudesta. 2008 Georgian sodan yhteyteen liittyi paljon palvelunestohyökkäyksiä. Tämä oli ensimmäinen kerta, kun perinteisten sotatoimien rinnalla esiintyi laajamittainen verkko-operaatioiden sarja. Kyberuhkat nähdään täydentävänä sodankäyntimuotona kaikille muille sodankäynnin muodoille. Luultavasti kybersodankäynnin menetelmiä käytettäisiin sotilasoperaatioiden rinnalla sotilas sekä siviilikohteisiin niiden lamauttamiseksi. Parhaimmillaan tai pahimmillaan kyberhyökkäyksillä kyetään tuottamaan yhteiskunnalle häiriötilanteita ilman, että tarvitsee käyttää fyysistä aseistusta (Puolustusministeriö, 2012, 20).

Vuonna 2009 maailmalla levisi haittaohjelma Conficker. Se onnistui saastuttamaan arvioilta seitsemän miljoonaa tietokonetta noin kahdessasadassa valtiossa. Sillä oli vaikutusta myös sotilaalliseen toimintaan. Ranskan merivoimien tietoverkko sai tartunnan, joka esti lentotoiminnan useissa lentotukikohdissa. Isossa-Britanniassa puolustushallinto raportoi myös saastuneista keskeisistä järjestelmistä. Samoin oli Saksan asevoiminen laita, sieltä raportoitiin saastuneista työasemista. Vuonna 2010 ilmaantui mullistavin haittaohjelma tähän asti, Stuxnet. Erilaisen siitä muihin verrattuna tekee, että se on räätälöity ja toimii vain, kun tietyt tarkat kriteerit täyttyvät. Tämän haittaohjelman kohteena oli Siemensin toimittama sentrifugien ohjauslogiikka. Kyseinen haittaohjelma levisi pääosin Iranissa, jossa se aiheutti tuhoa uraanirikastamossa. Vuonna 2011 havaittiin

jälleen uusi haittaohjelma, Duqu. Kyseisenä vuonna esiintyi paljon haktivistitoimintaa. (Candolin, 2012, 7-8).

Kuvasta 3 voidaan nähdä kyberaseiden evoluutio, joista Stuxnet haittaohjelma on ollut tähänastisista kehittynein. F-Securen tutkimusjohtaja Hyppönen Mikko on sanonut Stuxnet viruksen olevan ainutlaatuinen. Hän kuvasi sitä vuosikymmenen tärkeimmäksi haittaohjelmaksi. Hyppönen rinnasti tämän haittaohjelman kehityksen samaan kuin, jos kala nousisi kuivalle maalle. Virukselle oli erikoista se, että sillä oli vain yksi kohde. Kohteena oli teollisuus ja sen suljettu verkkoympäristö. Stuxnet virus ei levinnyt internetin välityksellä vaan ainoastaan muistitikkujen avulla. Se ei sotkenut tietokoneita vaan häiritsi tehtaan laitteiden toimintaa (Hyppönen, 2010).

Kaikissa kyberuhkissa on yhteisenä tekijänä se, että hyökkääjä on vaikeasti tunnistettavissa. Kyberuhkia voidaan aikaansaada niin monella tasolla. Niitä voidaan tuottaa valtiollisesti, eri tiedusteluorganisaatioiden avulla. Rikollisjärjestöt, yksittäiset hakkerit ja terroristit ovat myös useiden kyberhyökkäysten takana (Puolustusministeriö, 2012, 20).



Kuva 3, Kyberaseiden evoluutio, Turvallisuusforum

2.2 Psykologinen vaikutus

Yleisin yhteinen nimittäjä useimmissa terroristihyökkäyksissä on pelko. Pelkoa halutaan luoda yksittäisiin ihmisiin, ryhmiin ja yhteisöihin. Hyökkäyksillä voidaan luoda huomattavaa negatiivista julkisuutta ja taloudellista vahinkoa. Esimerkiksi vuonna 1999 Amazon.com – sivusto jouduttiin sulkemaan, kun sen palvelin joutui lukuisten palvelinhyökkäysten kohteeksi. Palvelinhyökkäykset sivustoa kohtaan levisivät julkisuudessa maailmanlaajuisesti. Kaikilla kyberhyökkäyksillä ei ole aina tarkoitus päästä suuriin taloudellisiin tappioihin. Kyberhyökkäyksillä haetaan usein haavoittuvia kohtia yrityksistä ja yleisistä palvelimista sekä nettisivustoista. Palvelunestohyökkäyksillä häiritään yritysten toimintaa ja sivustoja. (Janczewski & Colarik 2007, xv).

Tietokoneperusteisella hyökkäyksellä eli kyberhyökkäyksellä on yleensä tarkoitus luoda tuhoa ja sekasortoa. Hyökkäyksen tarkoitus on luoda samanlainen pelontunne, kuin mitä niin sanotusti normaali terroristihyökkäys saa aikaan. Tällaisia iskuja voivat olla lentokoneen putoaminen, suuret taloudelliset menetykset tai hyökkäykset jotka johtavat kuolemaan tai vakavaan vammautumiseen (Kramer, Starr, Wentz 2009, 438).

Katharina Candolin mietiskeli blokissaan kyberin aiheuttamaa mahdollista pelkoa. Hän miettii, että voiko virtuaalisen maailman kautta tullut verkkohyökkäys, joka ei näy, ei kuulu, eikä haise, aiheuttaa samanlaisen pelon tunteen kuin fyysinen hyökkäys (Kyberturvallisuus.blogspot, 2011)?

Seuraava lainaus on Al Qaidan As Sahab Media säätiön julkaisemalta videolta vuodelta 2011.
"Hacking on the Internet is one of the key pathways to Jihad, and we advise the Muslims who possess the expertise in the field to target the websites and the information networks of big companies and government agencies of the countries that attack Muslims, and to focus on the websites and networks that are managed by the media center that fight Islam, Jihad and mujahideen." (Cebul 2011, 1)

Yleensä pelkoa herättää aina, kun puhutaan ääri-islamistien toiminnasta. Heidän aatteensa on niin kirkas ja he näkevät tavoitteensa selkeästi. He eivät koe syyllisyyttä saadessaan aikaan tuhoa viattomien siviilien keskuudessa, koska he edustavat ääri-islamisteille länsimaalaisuutta ja vääräuskoisuutta. Samankaltainen pelko esiintyy varmasti myös monissa muissakin yhteiskuntamme asukkaissa. Toisaalta media on osittain syyllinen alati kasvavaan pelkoon. Median kautta on syö-

tetty informaatiota, siitä että terrorismi vaanii kaikkialla uhaten meitä ja elämänmuotoamme (Huhtinen, Rantapelkonen 2006, 145).

Jokainen tietokoneiden käyttäjä on varmasti jossain vaiheessa kokenut epävarmuutta. Jos ei välttämättä kuitenkaan pelkoa siitä, että onko tietokone saastunut viruksella tai ovatko pankkitiedot säilyneet vain henkilökohtaisessa käytössä. Nettipankissa asioidessa yleensä pohditaan, että säilyvätkö vähät rahavarannot omassa käytössä vai voiko joku tunkeutua nettitietoihin ja siirtää rahoja omiin käyttötarkoituksiinsa. Suuremmalla mittakaavalla pelko voi olla aiheellistakin. Se että viedäänkö nettipankin käyttäjältä rahat, ei vielä horjuta yhteiskuntaa. Se horjuttaa ainoastaan yhteiskunnan kansalaisten uskoa pankkijärjestelmään. Yhteiskunnan korkeammilla tasoilla pelätään suurempia asioita, kuten The U.S. Cyber Consequences Unit johtaja ja pääekonomisti Scott Borg on seuraavasti lausunut:
"If you shut down power for about three days," he says, "it causes very little damage. We can handle a long weekend. But if you shut down power for longer, all kinds of other things begin to happen. After about 10 days the curve levels off with about 72% of all economic activity shut down. You don't have air conditioning in the summer; you don't have heating in the winter. Thousands of people die." (Stephens 2009).

Terroristit hyödyntävät kyberavaruutta aiheuttaakseen häiriöitä (Janczewski & Colarik 2007, 2). Suoranaisesti Suomi ei ole tällä hetkellä minkään toimivan terroristijärjestön kohde. Uhka on kuitenkin olemassa, koska Suomi mielletään osaksi länsimaita ja arvoja joita ne edustavat. Tulevaisuudessa on mahdollista, että isku Suomea kohtaan voidaan nähdä ääriliikkeiden kannalta hyväksyttävänä iskuna länsimaailmaa vastaan. Mahdollisissa iskuissa on pahinta niiden aiheuttama pelko ja epävarmuus (Aakko, Nordberg, Kantolahti, Kulmala, Putkiranta, Sillanpää, Toveri ja Visakorpi 2003, 36–37).

Fortumin yritysturvallisuusjohtajan Juha Härkösen mukaan virukset ja madot ovat yhä suurempi uhka automaatiojärjestelmille. Teollisuusjärjestelmät ovat aikaisemmin toimineet suljetuissa järjestelmissä. Järjestelmät kuitenkin käyttävät samankaltaista pohjaa kuin mitä toimistopuolen laitteissa käytetään ja tämä helpottaa haittaohjelmien siirtymistä myös suljetun järjestelmän puolelle, kuten Stuxnet-viruksen kohdalla tapahtui. (Härkönen, 2010).

Ylen MOT-ohjelmassa maanantaina 11. maaliskuuta 2013 keskusteltiin asiantuntijoiden voimin yhteiskunnan haavoittuvuudesta. Siinä nimettiin Suomen haavoittuvimmaksi osaksi sähköverkko.

Aapo Cederberg, joka toimii Turvallisuuskomitean pääsihteerinä, mainitsi mahdollisen kyberiskun kohdistuvan sähköverkkoon ja edeltävän mahdollista fyysistä iskua. Hän totesi, että poliittinen kynnys on madaltunut huomattavasti tämänkaltaisten iskujen toteuttamiseen (Yle Mot).

Kun asiaan perehtyneet tietoturva-asiantuntijat myöntävät järjestelmässä olevat aukot ja sitä kautta mahdollisuuden sabotoida yhteiskunnan toimintaa niin voiko kyseinen asia olla herättämättä pelkoa?

Maailma ei ole koskaan aikaisemmin ollut näin yhtenäinen ja monikulttuurillinen kuin se on tällä hetkellä. Sosiaalinen media yhdistää ihmisiä kielistä ja paikallisista tavoista riippumatta. Etäisyyttä voidaan venyttää tai supistaa kyberavaruudessa reaaliaikaisesti. Se ei välttämättä ole huoletonta. Kyberavaruuden mahdollisuudet ovat kahteen suuntaan, hyvään ja pahaan. Tässä informaatioympäristössä rauhan, kriisin ja sodan väliset rajat hämärtyvät. Samalla sotilaallisen toiminnan, sotilaan sekä aseen määrittäminen sotilas- ja siviilikohteiden erottamisen välillä vaikeutuvat. Toiminnan rajaaminen ainoastaan asevoimien sekä verkossa tapahtuvan rikollisuuden ja toisen valtion tekemän hyökkäyksen erottamiseksi toisistaan on vaikeaa.

Sisäisen ja ulkoisen turvallisuuden rajan hämärtyessä, sotilaallisen ja siviilialojen yhteistyön merkitys korostuu. Verkostoitumiskehityksen seurauksena yhteiskunnan tärkeät toiminnot sekä kansalaisten mielipiteet ovat helposti saatavilla sosiaalisten verkostojen ja median välityksellä. Tietoverkkosodankäyntiä ja psykologisia operaatioita on helppo suunnata yhteiskuntaa vastaan yksilöiden kautta. Sosiaalisten medioiden (Twitter, Facebook, Youtube jne.), jotka ovat suosittuja ihmisten keskuudessa, on helppo vaikuttaa mielipiteisiin ja ajatuksiin. Sosiaaliset mediat ovat mahdollistaneet niin sanotun massavaikuttamisen. Vaarallista sosiaalisen median käytössä on varomattomuus ja liian sinisilmäisyys. Sosiaalisen mediaan lisätty tieto saattaa olla lisätty sellaisessa valtiossa, missä lainsäädäntö on erilainen kuin Suomessa. Tietoturva ja tietosuoja-asiat eivät ole lainsäädännöllisesti jokaisessa valtiossa samanlaiset.

Informaation leviäminen sosiaalisessa mediassa on nopeaa, sillä Facebookillakin on Suomessa noin kaksi miljoonaa käyttäjää. Nopeus lisää psykologisen vaikuttamisen tehokkuutta. Huhut ehtivät levitä mediassa nopeammin kuin viranomaiset ehtivät niitä korjaamaan. Riski muodostuu siitä, että mitä pidempään huhut ehtivät vaikuttamaan sosiaalisen median ja ihmisten keskuudessa, sitä laajemmalle virheellinen tieto leviää sekä muuttuu jo siinä vaiheessa todenperäiseksi. So-

siaalinen media antaa mahdollisuuden keskusteluille ja ajattelulle provosoivilla keskusteluilla. Se kuitenkin mahdollistaa myös tiedustelun ja ennakkovaroituksen organisaatioiden näkökulmasta (Puolustusvoimat, psykologinen puolustus).

Vastaavanlaisesta tilanteesta on usein käytetty esimerkkinä Orson Wellesin ohjaamaa radiokuunnelmaa vuodelta 1938. Kuunnelma herätti kuulijoissaan suurta pelkoa ja lietsoi voimakasta joukkohysteriaa. Huolimatta siitä, että ohjelman alussa mainittiin sen olevan kuunnelma, viidesosa kuulijoista uskoi lähetyksen todeksi. Monet yrittivät jopa itsemurhaa ja suuri joukko ihmisiä pakeni paniikissa. Kuunnelma aiheena oli avaruusolentojen invaasio Englantiin (Lindfors, Yle 2008).

Tämä osoittaa sen, että kuinka jokin asia, mikä esitetään tiedotusvälineessä uskottavasti, voi horjuttaa järkevänkin ihmisen turvallisuuden tunnetta. Turvallisuus voidaan ymmärtää tilana, jossa asiat koetaan varmana eli ne ovat todellisia ja voivat liittyä mihin tahansa olemisen maailmaa koskevaan asiaan (Huru, Väyrynen 2004,64). Tässä Wellesin Maailmojen sota esimerkissä kyseessä oli radiokuunnelma, joka horjutti ihmisten turvallisuutta todenperäisyydellään. Vastaavanlainen tapaus voi toimia ihan yhtä uskottavasti internetinkin välityksellä.

3. KANSALLINEN KYBERSTRATEGIA

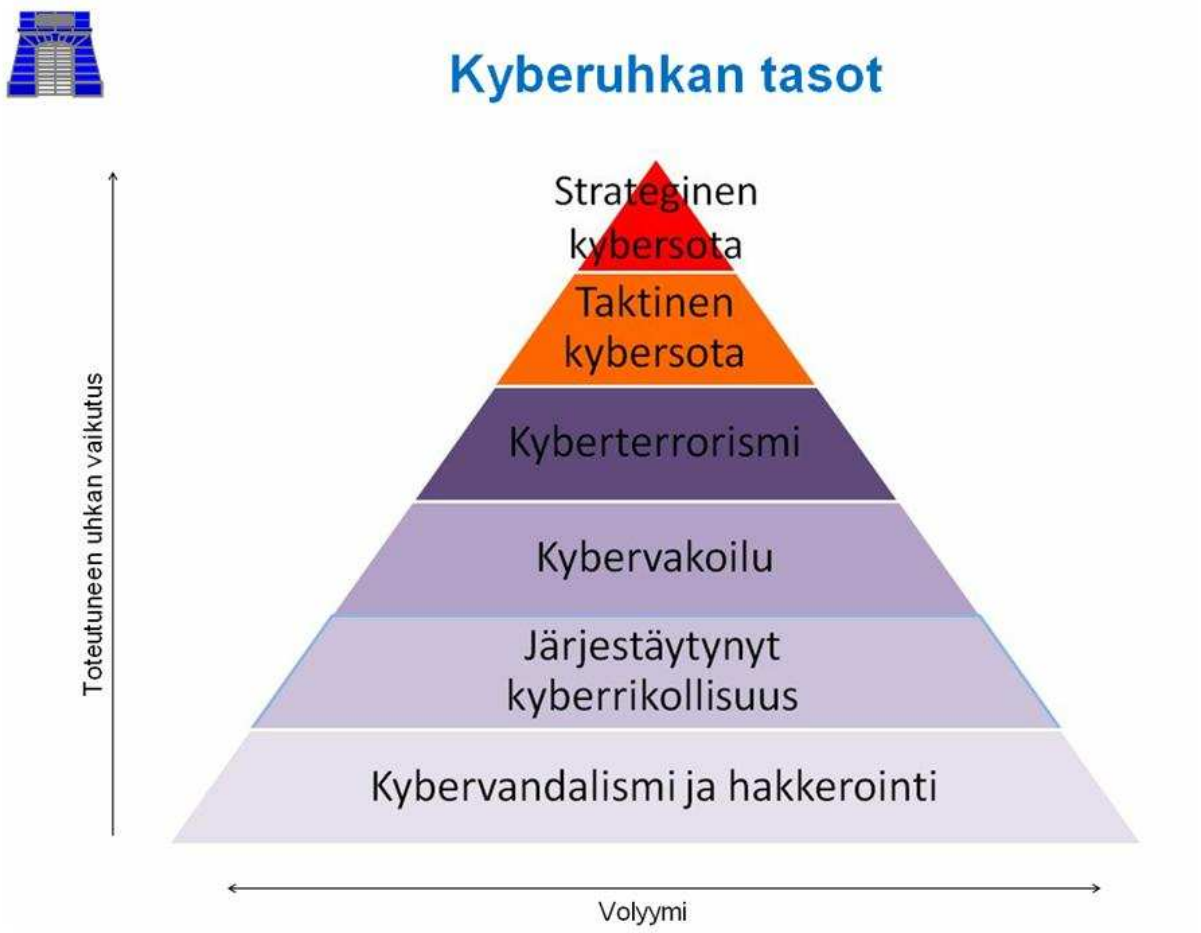
” Kyberturvallisuuden tarpeellisuus on yleisesti hyväksytty – onhan elämäntapamme ja vapautemme tehdä asioita suurelta osin riippuvainen elektromagneettisten järjestelmien tiedoista ja toimivuudesta. Kyberstrategian avulla valtiot ja järjestöt pyrkivät edistämän kyberturvallisuutta.” (Kerttunen, 2013, 14)

Kyberstrategian valmistelu ei ole ollut vaivatonta, koska kyberstrategian määritelmät ovat niin poikkeavia eri aloilla ja yhteisöillä. Ennen kansallisen strategian syntymistä on työryhmän pitänyt sopia yhteiset pelisäännöt ja termit mitä tullaan käyttämään. Termeissä koettiin ongelmia, sillä puolustusvoimille kyberstrategia tarkoitti kybersotaa, ulkoministeriö olisi puhunut diplomatiasta, poliisit järjestäytyneestä rikollisuudesta, valtionvarainministeriö mielsi sen liittyvän julkisiin palveluihin ja kriittisen infrastruktuuriin, liikenne ja viestintäministeriö pitivät asiaa jo entuudestaan omanaan. Kaikki ajankäyttö mitä työryhmä käytti terminologian yhteensovittamiseen ja asioiden suunnitteluun on kannattanut. Työryhmän työskentelyn lopputuotoksena on saatu aikaan kansallinen kyberstrategia (Ståhle 2013, 9).

Kyberturvallisuusstrategian syntyyn on vaikuttanut yhteiskunnan kokonaisturvallisuus. Turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä ja elintärkeät toiminnot on kyettävä turvaamaan kaikissa olosuhteissa. Kyberuhka on tiedostettu uhka ja se voi pahimmillaan laajaalaisesti vaikuttaa yhteiskunnan elintärkeisiin toimintoihin. Sähköiset palvelut ja tietoverkot muodostavat kokonaisuuden, jonka varassa yhteiskunta toimii. Tähän kokonaisuuteen kohdistuvat hyökkäykset muodostavat vakavan kyberuhkan. Vuodenvaihteessa 2011 – 2012 esiintyneet voimakkaat talvimyrskyt saivat aikaan laajoja voimahuollon ongelmia. Voimahuollon ongelmista eli energiansaannin heikkoudesta tai sen puutteesta kokonaan seurasi tietoverkkojen ja – järjestelmien häiriöitä. Nämä häiriöt olivat luonteeltaan sen kaltaisia, että samankaltaisia ongelmia voidaan aiheuttaa myös kyberhyökkäyksillä. Kansallinen kykymme muodostaa ja ylläpitää yhteiskunnan elintärkeiden toimintojen kokonaisuutta kyberturvallisuudessa ja toimintojen ohjausta poikkeusolosuhteissa vaatii kehitystä. Tästä johtuen voimme vastata konkreettiseen ja alati kasvavaan kyberuhkaan. Tästä syystä on laadittu ensimmäinen kansallinen kyberturvallisuusstrategia, joka julkistettiin tammikuussa 2013 (Turvallisuus ja puolustusasian komitea 2012, 1-3).

Suomen kyberturvallisuusstrategialla pyritään vastamaan yhteiskunnan muutokseen, joka johtuu lisääntyneestä tietointensiivisyydestä, ulkomaisen omistuksen kasvusta Suomessa sekä toimintojen ulkoistamisesta. Tieto- ja viestijärjestelmät muodostavat keskinäisen kiinteän integraation. Tietoverkot ovat jokaiselle kansalaiselle avoimet ja yhteiskunta on entistä enemmän riippuvainen sähkönkulutuksesta. Sähköriippuvaisuus asettaa uusia vaatimuksia yhteiskunnalle ja elintärkeiden toimintojen turvaamiselle normaalioloissa, sekä normaaliolojen häiriötilanteissa että poikkeusoloissa.

Kyberturvallisuusstrategiaa varten on kyberuhka pitänyt määritellä tarkasti. Kyberuhka voidaan jakaa eri tasoihin, joten se, kuten muutkin uhkat eivät ole yksiselitteisiä tai suoraviivaisia. Kuvassa 4. on esitetty kyberuhkan eri toimintatasot.



Kuva 4. Kyberuhkan tasot, Benson 2012

Kybertoimintaympäristöön kohdistuvia uhkia pidetään nyt vaikutuksiltaan vaarallisempina yksittäisten ihmisten, yritysten ja koko yhteiskunnan kannalta. Kybertoimintaympäristö pyritään tekemään turvalliseksi, joka puolestaan helpottaa yksilöiden ja yritysten toiminnan suunnittelua sekä tätä kautta lisää taloudellista toimintaa. Hyvä ja turvallinen toimintaympäristö lisää Suomen houkuttelevuutta kansainvälisenä investointikohteena. Kyberturvallisuudesta on myös kehittynyt uusi ja aina vahvistuva liiketoiminnan alue.

Suomen kyberturvallisuusstrategiassa määritellään keskeiset toimintalinjat ja tavoitteet, joilla vastataan haasteisiin joita kybertoimintaympäristössä esiintyy. Tämä strategia antaa linjaukset ja toimenpiteet joiden avulla Suomi kykenee hallitsemaan kybertoimintaympäristön erilaisia haittavaikutuksia, sekä toipumaan kuin myös vastaamaan niistä. Kyberturvallisuusstrategia on osa yhteiskunnan turvallisuusstrategiaa. Se noudattaa yhteiskunnan turvallisuusstrategiassa olevia periaatteita ja määritelmiä. Strategia ottaa huomioon periaatepäätöksen kokonaisturvallisuuden järjestelyistä. Kyseisen strategian avulla ei lisätä uusia toimivaltuuksia viranomaisille tai muille toimielimille. Siinä kuvataan visio, toimintamalli ja strategiset linjaukset. Erillinen toimeenpanoohjelma, mikä sisältää käytännön toimenpiteet, on vasta valmisteilla.

Strategiassa on laadittu visio siitä, mitä Suomen on kyettävä tekemään kyberturvallisuuden ollessa uhattuna. Suomen on kyettävä suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan. Elintärkeitä toimintoja on muun muassa valtion johtaminen. Valtion johtamisella tarkoitetaan eduskunnan, tasavallan presidentin ja valtioneuvoston yhteistyötä. Tavoitetilassa johtaminen on näiden kolmen sekä ministeriöiden toimintaa kansallisten voimavarojen käyttämiseksi turvallisuustilanteiden edellyttämällä tavalla. Johtamiselle luodaan tarvittavat toimintaedellytykset päätöksen tekoon ja yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi (YETTS 2006, 13).

Kansainvälinen toimintakyky on Suomelle tärkeä. Se on kiteytettynä kykyä ylläpitää yhteyksiä ulkovaltoihin sekä varmistaa Suomen kantojen välittyminen Euroopan unionin toimielimissä ja kansainvälisten yhteenliittymien toiminnassa. Kansainvälinen toimintakyky on myös Suomen kansalaisten auttamista ulkomailla ja ulkomaankaupan yhteyksien turvaamista (YETTS 2006, 14).

Suomen puolustuskyky muodostaa oman kokonaisuutensa elintärkeistä toiminnoista. Se on valtakunnan sotilaallista puolustamista ja yhteiskunnan voimavarojen suunnittelua siten, että Suomeen kohdistuvan sotilaallisen uhka saadaan ehkäistyä sekä torjuttua (YETTS 2006, 15). Sisäinen turvallisuus pitää sisällään ne toimenpiteet, joilla oikeusvaltion toimintaedellytykset turvataan, ennaltaehkäistään sekä torjutaan Suomeen ja väestöön kohdistuvia rikoksia, onnettomuuksia kuin myös muita häiriöitä (YETTS 2006, 16). Sisäisen turvallisuuden tarkoitus on myös se, että Suomi on Euroopan turvallisin maa, jossa yhteiskunnan jäsenet toimivat yhdenvertaisina ja oikeudenmukaisuus koskettaa kaikkia (Benson 2011, 3).

Talouden ja infrastruktuurin toimivuus on tärkeää, jotta väestön ja elinkeinoelämän mahdollisuuksia perustarpeiden tyydyttämiseen taloudellisen vaihdannan sekä riittävän vahvan julkisen talouden rahoitusaseman saadaan toimivaksi. Tähän kuuluu infrastruktuurin ylläpitämistä, julkisen talouden toimintaedellytysten, rahoitusmarkkinoiden ja vakuutusalan toiminnan turvaamista. Myös sähköiset tieto- ja viestintäjärjestelmät, kuljetusten turvaaminen, yhteiskunnan taloudellisten perustoimintojen ylläpitäminen, työvoima, korkeatasoinen koulutus sekä ympäristömuutosten havainnointi ja niihin sopeutuminen liittyvät tähän (YETTS 2006, 16).

Väestön toimeentuloturva ja toimintakyky on yksi osa-alue myös elintärkeistä toiminnoista. Se on yhteiskunnan kykyä tuottaa väestön sosiaaliturva sekä sosiaali- ja terveydenhuoltopalvelut. Se on syrjäytymisen ennaltaehkäisyä, yhteiskunnan rauhan edistämistä sekä väestön itsenäistä selviytymistä ja toimintakykyä (YETTS 2006, 19). Henkinen kriisinkestävyys on nimensä mukaisesti kyky kestää turvallisuustilanteiden aiheuttamat paineet ja selviytyä niiden vaikutuksilta. Kriisinkestävyyden kykyä ylläpidetään sosiaalisen eheyden viestinnän, opetuksen ja muiden yhteisten toimien avulla (YETTS 2006, 20).

Kansalaisille, viranomaisille ja yrityksille on luotava mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamisen yhteydessä syntyvää osaamista sekä kansallisesti ja kansainvälisesti. Tavoitteena strategiassa on myös, että vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden häiriötilanteiden hallinnassa. Suomella on vahva ja haastava visio, että vuonna 2016 olemme edelläkävijä kyberuhkien varautumisessa ja hallinnassa. Visio ei ole kuitenkaan temmattu tuulesta, sillä Suomella on monia seikkoja, jotka edesauttavat korkealaatuisen kyberstrategian aikaansaannissa (Suomen kyberturvallisuusstrategia 2013, 3).

Viime sodista lähtien meillä on ollut huoltovarmuus – ja varautumisajattelua, joka edesauttaa yhteiskuntaa laajoihin poikkeusoloihin. Poliittiset foorumit, kuten UTVA eli ulko- ja turvallisuuspoliittinen valiokunta on olemassa koordinointia varten. Turvallisuus ja puolustuskomiteaa voidaan luontevasti käyttää kyberturvallisuusstrategian työn ohjaamiseen ja seurantaan. Suomessa on järjestetty TIETO-harjoituksia, jotka ovat useiden vuosien ajan keskittyneet tietoverkkoihin. Suomessa on myös hyvä ja vakiintunut käytäntö viranomaisyhteistyölle. Valtiona Suomi on riittävän pieni ja kompakti, jotta asiat hoituvat kansallisella tasolla kohtuullisessa ajassa. Suomi on myös vuosien ajan ollut korkean teknologian maa ja erittäin teknologiamyönteinen. Osaamista löytyy kyberturvallisuuden vaatimiin teknisiin ratkaisuihin niin kotimaan tarpeita kuin myös vientiä ajatellen Pitkäjänteinen tietoturva yhteistyö ministeriöissä, virastoissa sekä yrityksissä ovat luoneet hyvän ja laadukkaan pohjan kyberturvallisuusstrategian tekemiselle kuin sen jämäkälle toteutumiselle (Benson 2011, 8).

Suomen kyberstrategiassa on otettu huomioon kybertoimintaympäristön nopeasti tapahtuvat muutokset ja se, että muutosten vaikutukset ovat vaikutuksiltaan vaikeasti ennakoitavia. Informaationteknologian kehityssykli on lyhyt ja sama koskee erilaisia kyberhyökkäysmuotoja sekä haittaohjelmia. Tästä muodostuu haaste ja kyberuhkiin varautuminen sekä torjunta edellyttävät yhteiskunnan kaikkien osapuolten nopeaa, läpinäkyvämpää kuin myös entistä paremmin koordinoitua toimintaa yhdessä tai erikseen (Suomen kyberturvallisuusstrategia 2013, 4).

Suomessa kyberturvallisuuden ylimmän tason muodostaa valtioneuvosto. Sen tehtävänä on poliittinen ohjaus, strategiset linjaukset sekä voimavaroista ja toimintaedellytyksistä päättäminen. Valtioneuvostolla ja eri toimijoilla on oltava käytettävissään luotettava sekä ajankohtainen kybertuvallisuuden tilannekuva. Ilman näitä johtamisesta muodostuu hankalaa ja häiriötilanteiden hallinta muodostuu vaikeaksi. Ministeriöt ja hallinnonalat vastaavat kyberturvallisuudesta ja häiriötilanteiden hallinnasta. Ministeriöiden strategiset tehtävät ja niihin liitetyt kehittämistarpeet perustuvat tunnettujen kyberuhkien analysointiin sekä niistä muodostettuihin häiriötilanteiden hallinnan vaatimuksiin. Jokaisen ministeriön tehtävä on toimivaltansa puitteissa huolehtia siitä, että tavoitetilojen perusteella laaditut strategiset tehtävät toteutetaan (Suomen kyberturvallisuusstrategia 2013, 4).

Kyberuhkien yhteydessä voidaan puhua kyberresilienssistä, joka tarkoittaa kyberuhkien sietokykyä. Sietokyky mitoitetaan siten, että kyetään luomaan kokonaisturvallisuuden päämäärien mukaan varautumis- ja ennakointikykyä, toimintakyky kyberhäiriötilanteissa sekä toipumis- ja palautumiskyky kyberhäiriöiden jälkeen. Suomen kyberturvallisuuden toimintamalli jaetaan kahdeksan periaatteen mukaan. Periaatteet ovat:

– Pääsääntöisesti kyberturvallisuusasiat kuuluvat valtioneuvoston toimivaltaan. Tehtävät on säädetty eri ministeriöiden toimialoille. Ministeriöt vastaavat omalla toimialueellaan kyberturvallisuuteen liittyvistä asioista.

– Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta. Toimintamalli noudattaa yhteiskunnan turvallisuusstrategian määrittämiä periaatteita ja toimintatapoja.

– Kyberturvallisuus perustuu yhteiskunnan tietoturvallisuuden järjestelyihin. Sen edellytys on jokaisen toimijan, joka on kyberturvallisuusympäristössä, tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut.

– Toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedonhankinta-, analysointi-, keruujärjestelmään, yhteiseen sekä jaettuun tilannetietoisuuteen että kansalliseen kuin myös kansainväliseen yhteistoimintaan varautumisessa. Perustetaan kyberturvallisuuskeskus sekä koko yhteiskunnan ympärivuorokautinen tietoturvatoiminnan kehittäminen.

– Järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja ennalta sovittuun yhteistyöhön. Toimijoilta vaaditaan kykyä ymmärtää strategisia periaatteita ja niiden noudattamista kyberturvallisuuteen tähtäävien toimien kehittämisessä sekä johtamisessa.

– Kyberturvallisuutta rakennetaan toiminnallisten ja teknisten vaatimusten perusteella. Sen lisäksi panostetaan kansainväliseen yhteistoimintaan ja osallistutaan kansainväliseen tutkimus- ja kehittämistoimintaan sekä harjoitustoimintaan.

– Kyberturvallisuuden kehittämisessä keskitytään kybertoimintaympäristön tutkimukseen, työllistymiseen, koulutukseen ja tuotekehitykseen. Tämän tarkoitus on mahdollistaa Suomen kehitys yhdeksi maailman johtavaksi kyberturvallisuuden valtioksi.

– Jotta varmistetaan kyberturvallisuuden kehitys, huolehditaan voimassaoleva lainsäädäntö ja kannustimet, jotka tukevat yritystoimintaa sekä kehittymistä. Kehittyminen kyberturvallisuusalalla kehittyy yritystoiminnan kautta

(Suomen kyberturvallisuusstrategia 2013, 5).

Kansallinen kyberstrategia pitää sisällään linjauksia, joilla kehitetään strategiaa. Linjaukset luovat edellytykset, jotta kansallinen visio saadaan toteutettua eli Suomi on johtava maa kyberturvallisuudessa vuonna 2016. Kyberturvallisuusstrategian toteutuminen varmistetaan erikseen laaditulla toimeenpano-ohjelmalla. Toimeenpano-ohjelma koostuu laadituista suunnitelmista mitä eri toimijat ja hallinnonalat ovat laatineet sekä suunnitelmien pohjalta laadituista poikkihallinnollisista toimenpiteistä. Strategisten linjausten toimeenpano vahvistaa julkisen ja yksityisen sektorin välistä yhteistyötä. Yhteistyön avulla saadaan paremmin palveltua yhteiskuntaa ja tuettua toimijoita, jotka tuottavat elintärkeitä toimintoja. Strategian päämäärä on, että eri toimijat voivat toimia sekä arjessa, että häiriötilanteissa. Kaikki tämä perustuu pitkäjänteisyyteen ja riittävään suorituskykyjen kehittämiseen. Toiminnan pitää olla oikea-aikaista ja joustavaa sekä elintärkeiden toimintojen tulee sietää mahdollisia häiriötilanteita (Suomen kyberturvallisuusstrategia 2013, 6).

Viranomaisten suorituskykyä kehitetään toimivaltaisten ministeriöiden johdolla. Suorituskyvyn kehittämisessä ja käytössä on otettava huomioon hallinnon eri tasot sekä elinkeinoelämän että järjestöjen rooli. Yhteistoimintaelimeksi perustetaan turvallisuuskomitea, jonka tehtävät säädetään erikseen (Suomen kyberturvallisuusstrategia 2013, 6).

Kyberturvallisuusstrategiassa eri linjauksia on kaiken kaikkiaan kymmenen. Linjauksia ovat:

1. Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.
2. Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.
3. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten sekä organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja – häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.
4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia sekä sitä hyödyntäviä rikoksia.
5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.
6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden sekä yhteistyöfoorumeiden toimintaan.
7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja – ymmärrystä.

8. Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.
9. Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät sekä palvelumallit kuin myös yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.
10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.
(Suomen kyberturvallisuusstrategia 2013, 7-11).

Suomeen perustettavan kyberturvallisuuskeskuksen avulla parannetaan elintärkeiden toimintojen turvaamiseen osallistuvien tahojen tilannetietoisuutta ja tilanneymmärrystä. Keskuksen tarkoitus on palvella viranomaisia, elinkeinoelämää ja muita toimijoita. Keskuksen tuottamilla palveluilla kehitetään kyberturvallisuutta ja ylläpidetään tilannetietoisuutta. Toimintatavoista sovitaan osana kyberturvallisuusstrategian toimintasuunnitelmassa. Palvelun ydin on kybertilannekuvan luomisessa ja jakamisessa kiinteässä yhteistyössä turvallisuuskeskusta tukevan verkoston kanssa. Keskus muodostetaan nykymuotoisen CERT-FI toiminnon ja GOV-CERT toiminnon yhdistämisellä ja varaamalla toteuttamiseen tarvittavat lisäresurssit (Suomen kyberturvallisuusstrategian taustamuistio 2013, 9-10).

Nykymuotoinen CERT-FI on viestintävirastossa toimiva kansallinen tietoturvaviranomainen. Tietoturvaviranomaisen tehtäviä ovat tietoturvaloukkausten ehkäisy, havainnointi ja syntyneiden ongelmien ratkaisua sekä erilaisista tietoturvauhista tiedottaminen. CERT-FI on aloittanut toimintansa jo vuonna 2002, joten täysin tyhjästä ei tarvitse uutta turvallisuuskeskusta rakentaa (Talka, 2013, 5).

GOV-CERT on puolestaan kymmenen eurooppalaisen tietoturvaviranomaisen yhteistyöverkosto. Yhteistyö on lähtenyt liikkeelle ajatuksesta, että jokaisen suvereenin valtion on kyettävä puolustamaan itseään verkostohyökkäyksiä vastaan (Viestintävirasto, Signaali 2011, 18).
Nämä kaksi tietoturvakanavaa yhdistämällä saadaan varmasti laadukas sekä toimiva kokonaisuus, joka palvelee suomalaista yhteiskuntaa ja toimii hyvässä vuorovaikutuksessa kansainvälisten muiden keskuksien kanssa.

3.1 Kyberturvallisuusstrategioita maailmalla

Suomi ei ole ainoana valtiona maailmassa luonut kyberturvallisuusstrategiaa vaan strategioita löytyy muistakin maista. Strategioissa on havaittavissa yhtäläisyyksiä ja eroja, mutta pääasiallinen tarkoitus strategialla on luonnollisesti parantaa oman valtionsa kyberturvallisuutta.

Viron kyberturvallisuusstrategia on julkaistu vuonna 2008 eli vuosia aikaisemmin kuin Suomi on laatinut oman kansallisen strategiansa. Viron kyberturvallisuusstrategian laatimiseen on selkeästi syynä valtion vuonna 2007 kokema kyberhyökkäysten aalto, joka kosketti koko valtiota. Koordinoidut kyberhyökkäykset valtion virastoja, pankkeja, teleyhtiöitä ja mediaa kohtaan paljastivat kuinka haavoittuvia yhteiskunnan tietojärjestelmät ovat. Strategian avulla pyritään vastaamaan kasvaviin kyberuhkiin, koska ne eivät saa hidastaa yhteiskunnan ja informaatioteknologian kehitystä. Viron kyberturvallisuusstrategiassa on myös määritetty periaatteita ja suuntalinjoja, joilla parannetaan kyberturvallisuutta. Linjauksissa mainitaan muun muassa, että kyberturvallisuus on otettava rutiinimaisesti mukaan kansallisen turvallisuuden suunnittelussa. Strategiassa peräänkuulutetaan yhteistyötä yleisen ja yksityisen sektorin välillä, eli siis samaa kuin Suomen laatimassa strategiassa. Kansainvälinen yhteistyö on ymmärretty tärkeäksi osaksi strategian kehittämisessä, jotta turvallisuutta saadaan parannettua kansallisesti ja globaalisti. Viron strategia on laaja-alainen kokonaisuus, jossa otetaan kantaa kyberavaruuden uhkiin, lainsäädäntöön, kansainväliseen yhteistyöhön, tietoturvaan, asetetaan tavoitteita mitä kyberturvallisuudella tulee saavuttaa ja niin edelleen. (Estonia, Cyber Security Strategy, 2008).

Yhdysvaltojen kyberturvallisuusstrategiassa lähdetään asetelmasta, jossa todetaan, että ilman merkittävää muutosta turvallisuuden saralla ei voida vastata kyberturvallisuuden tuomiin kasvaviin uhkiin. Nykyinen tilanne on mahdollistanut rikollisten hyödyntää digitaalista infrastruktuuria satojen miljoonien dollarien edestä ja arkaluontoista sotilaallista tietoa on päätynyt vääriin käsiin sekä tekijänoikeusrikkomuksia on tapahtunut runsaasti. Yhdysvaltojen strategiassa on määritelty linjauksia, jotka ohjaavat parempaan kyberturvallisuuteen. Heidän strategiansa on samansuuntainen kuin Suomen. Strategiassa linjataan yhteistyön merkityksestä ja toteutuksesta. Kansainvälinen yhteistyö nähdään tärkeänä ja vahvuutena. Strategia mainitaan presidentin yhdeksi tärkeimmäksi prioriteetiksi. Strategialla on tarkoitus lisätä ihmisten tietoisuutta kyberturvallisuudesta ja sen riskeistä. Sen avulla on tarkoitus valmistautua kyberturvallisuuden aiheuttamiin häiriötiloihin,

edesauttaa julkisen ja yksityisen sektorin yhteistyötä tarjoamalla resursseja optimoidakseen noiden kahden sektorin panosta sekä sitoutumista kyberturvallisuuteen (Yhdysvallat 2009).

Alankomaat on saanut oman kyberstrategiansa vuonna 2012. Alankomaalaisten kyberturvallisuusstrategiassa rinnastetaan digitaalinen ulottuvuus (domain) samaan kuin maa, ilma, meri ja avaruus. Se on viides ulottuvuus sotilaallisissa toimissa. Tässä digitaalisuus ymmärretään niin sanotusti älykkyyden keinona/aseena ja sen kehittyminen on voimakasta. Laaja kyberhyökkäys yhteiskuntaa vastaan voi olla tuhoisa. Sen vaikutukset voivat olla samankaltaisia kuin terroristihyökkäyksessä, vaikuttaa laajasti yhteiskunnan järjestykseen ja aikaansaada yhteiskunnallisia häiriöitä. Alankomaalaiset ovat myös perustaneet tai perustamassa kansallista kyberturvallisuuskeskusta, joka koordinoi tiedustelua, viranomaisia ja mahdollisesti asevoimia. Heidän linjauksissaan määritellään kokonaisvaltainen lähestymistapa, jolla saavutetaan tavoitteet digitaalisessa ulottuvuudessa. Linjauksissa ohjeistetaan puolustusministeriön vahvistamista, jotta saavutetaan kyberstrategian asettamat tavoitteet. Heidän strategiassaan linjataan tiedustelut ja jopa mahdolliset hyökkäykset. Yhteistyön merkitys on huomattu ja sen tärkeys ymmärretty. Digitaalisen kehityksen nopeus vaatii innovatiivisyyttä ja mukautuvuutta puolustusministeriöltä, joka koordinoi turvallisuuskeskuksen kanssa kaikkea kyberstrategian osa-alueita. (Alankomaat 2012)

Edellä oli vain muutamia esimerkkejä kyberstrategioista, joita eri valtiot ovat julkaisseet. Edellä mainituista kolmesta esimerkistä kyberturvallisuusstrategiastakin voidaan havaita lukuisia yhtäläisyyksiä Suomen kansalliseen kyberturvallisuusstrategiaan. Kaikissa strategioissa ymmärrettiin yhteistyön, etenkin kansainvälisen yhteistyön merkitys. Kansainvälisyys nähdään voimavarana, joka samalla kehittää valtioiden omia kansallisia strategioita. Edellä mainituissa esimerkeissä valtiossa oli perustettu tai ainakin suunnitelmissa perustaa oma erillinen kyberturvallisuuskeskus, joka koordinoi lähes samankaltaisia asioita kuin Suomen vastaava. Yleinen tiedottaminen kyberuhkista ja – turvallisuudesta nähtiin erittäin tarpeellisena ja sen avulla annettavan tietämyksen ymmärrettiin olevan vain etu yhteiskunnalle.

Valtiot joutuvat miettimään lainsäädäntöään kyberturvallisuuteen liittyen, jotta tarvittavilla viranomaisilla on resurssit hoitaa omat määrätyt tehtävänsä. Toki erojakin kyberturvallisuusstrategioissa ilmeni. Esimerkkivaltiossa Alankomaissa, armeijan toimet ovat suuressa painoarvossa, kun puhutaan vastaamisesta ja suojautumisessa kyberhyökkäyksillä. Määritelmä eroja ilmenee myös jonkin verran, kuten edellä mainittu Hollanti määrittelee digitaalisuuden yhtenä elementtinä ja

ulottuvuutena sotilaallisessa merkityksessä. Suomessa ei ole keskustelut edenneet vielä sille tasolla, jossa mietittäisiin kyberhyökkäyksiin vastaamista aseellisin keinoin.

4. SUOJAUTUMINEN KYBERUHKAN ERI MUODOILTA

Turvallisuuden näkökulmasta kyberuhkat ovat kokonaisvaltaisia, rajat ylittäviä. Nämä uhkat ulottuvat kaikilla mahdollisille elämänaloille suomalaisessa tietoyhteiskunnassa. Kyberuhkat ovat kaikkien viranomaisten yhteinen huolenaihe ja tämä vaatii kokonaisvaltaista otetta yhteiskunnassa (Puolustusministeriö, 2012, 21).

Yhteiskunnan on kyettävä suojautumaan kyberuhkilta. Suojautumiselle on selkeä tarve, sillä CERT-FI raportoi vuoden 2012 vuosikatsauksessa palvelunestohyökkäysten ja haittaohjelmatartuntojen olleen kyseisen vuoden yleisimpiä tietoturvauhkia. CERT-FI -yksikköä työllistivät mediaan kohdistuneet palvelunestohyökkäykset, ohjelmistoissa ilmenneet erilaiset haavoittuvuudet, kiristyshaittaohjelmat ja tietomurrot. Vuonna 2012 CERT-FI yhteydenotoista, joita oli 4208, koski haittaohjelmia. Yhteydenotot olivat siis yksityisten henkilöiden tai muiden tahojen kautta tulleita yhteydenottoja ja avunpyyntöjä. Kasvua edelliseen vuoteen oli 10 prosenttia. Haittaohjelmien esiintyvyys on ollut nähtävissä jo vuodesta 2006. Tietomurtotapauksia yksikkö käsitteli 271. Tässäkin oli kasvua edelliseen vuoteen 74 prosenttia. Palvelunestohyökkäyksiä perusteltiin huomionhakuisuudella, sillä Suomen mittakaavassa palvelunestohyökkäykset olivat poikkeuksellisen laajoja. Ne kohdistuivat eri media-aloihin kuten Yleisradioon, Helsingin sanomiin MTV3:n palvelimiin (Viestintävirasto, CERT-FI, vuosikatsaus 2012, 2013).

Yhteiskunnan turvallisuusstrategiassa vuonna 2011 sanotaan, että uhkien, jotka koskevat väestöä, yhteiskuntaa ja valtiota, niiden hallinta edellyttää kaikkien osallistuvien toimijoiden tuntemat ja harjoittelemat yhteiset toimintatavat. (Yhteiskunnan turvallisuusstrategia 2011, 51).

Suojautuminen uhkilta vaatii erilaisten strategioiden muodostamista valtiolliselta taholta. Esimerkiksi Viron käyttämällä kyberstrategialla pyritään ensisijaisesti vähentämään luontaisia haavoittuvuuksia koko kansakunnan kyberavaruudessa. Tämä saavutetaan toteuttamalla kansallista toimintasuunnitelmaa ja aktiivista kansainvälistä yhteistyötä. Yhteistyö tehostaa samalla muiden maiden kyberturvallisuutta. (Estonian ministy of defence).

Kansainvälistyminen ja globalisaatio ovat aikaansaaneet tilanteen, jossa aiemmin kotimaassa sijainnutta teollisuutta on siirretty ulkomaille. Kansainvälistymisen myötä ovat yritysten omistussuhteet myös muuttuneet. Omistajaintressit ovat lisääntyneet ulkomaisomistuksen suuntaan. Kansainvälistymisen johdosta yhteiskunnallista tärkeää infrastruktuuria on siirtynyt ulkomaille. Siitä on tullut osa kansainvälistä infrastruktuuria ja se voi olla valtiollisen tai yksityisen omistamaa. Tämä lisää haasteita turvallisuuden valvonnalle ja vastuun ylläpitämiselle. Kohteet mitä pitää turvata, voivat sijaita kaukana maamme rajojen ulkopuolella. Ulkomaille siirtyminen aikaansaa tilanteen, jossa huomattava määrä tietoa ja taito on myös maamme rajojen ulkopuolella. Tästä johtuen yhteiskunnan valmius turvata elintärkeitä toimintoja kriisitilanteissa on vaikeutunut (Sallinen 2005, 98). Absoluuttiseen suojautumiseen ei ole vielä olemassa keinoja, vaikka meillä onkin käytössä järjestelmiä jotka havaitsevat tai torjuvat hyökkäyksiä ja niiden uhkia (Yhteiskunnan turvallisuusstrategia 2011, 66).

Elintärkeiden toimintojen turvaamiseen ei välttämättä enää riitä yhteiskunnan omat valtiolliset resurssit. Suojaamiseen on hyvä yrittää ottaa mukaan yksityistä sektoria, koska silläkin sektorilla on omistuksia Suomen valtion rajojen ulkopuolella. Ongelma tässä on yritysten voittojen tavoittelu. Elintärkeiden toimintojen turvaaminen ei aina ole kaupallisessa tarkoituksessa kannattavaa, joten julkisen vallan pitää saada sidottua yksityinen sektori paremmin yhteistyöhön mukaan. Julkinen valta katsoo, ettei toimivan yhteiskunnan ylläpitäminen ole täysin sen asia, koska toimiva yksityinen sektorikin muodostaa osan yhteiskunnasta (Sallinen 2005, 99).

Yritykset ovat lisänneet markkinointia ja kaupankäyntiä runsaasti internetiin. Sähköisen kaupankäynnin rooli kotitalouksissa korostuu entistä enemmän. Pitkälliset palvelunestohyökkäykset tällaisia yrityksiä vastaan voivat ajaa yrityksen konkurssiin. Nämä niin sanotut DoS-hyökkäykset ovat hankalia ja tekevät hyökkäysten havaitsemisen vaikeaksi. Näiltä suojautuminen on hankalaa, mutta ei mahdotonta. Näitä DoS-hyökkäyksiä voi käyttää sotilaallisessa tarkoituksessa hyökkäysmenetelmänä esimerkiksi ohjusten asemesta. Ensin pitää kuitenkin oppia havaitsemaan sekä puolustautumaan niiltä ja sen jälkeen voi hyödyntää tietotaitoaan monella eritavalla (McClure, Scambray, Kurtz 2002, 552).

Kuitenkaan hyväkään suojautuminen ei aina riitä, hyökkäyksiä voi silti tapahtua ja ne voivat läpäistä suojautumismekanismit. Tavoitteena pitää myös olla vahinkojen rajaaminen. Hyökkäys tulee havaita nopeasti, jotta se saadaan rajattua ja vahingot minimoitua. Hyökkäyksestä jää aina

todisteita, täysin puhdasta hyökkäystä ei olekaan. Todisteiden turvaaminen on tärkeää, jotta tekijät saadaan rikosoikeudelliseen vastuuseen ja todisteita tutkimalla yritys voi oppia tehdystä hyökkäyksestä. Mikäli organisaatio kykenee selvittämään kuinka ja miksi hyökkäys onnistui, se ehkäistä samankaltaisen hyökkäyksen tulevaisuudessa (Kajantie, 2009, 23).

4.1 Yksityishenkilön suojautumiskeinot

Tilastokeskuksen teettämän tieto- ja viestitekniikan käyttötutkimuksen mukaan internetin käyttö yleistyy enää hitaasti. Käyttäjien osuus 16–74 vuotiaasta väestöstä kasvoi vuonna 2012 yhden prosenttiyksikön nousten näin 90 prosenttiin. Käyttäjämäärä on huomattavan korkea. Tilastokeskuksen tutkimuksen mukaan verkkokaupan asiakkaiden määrä puolestaan kasvaa. Noin puolet suomalaisista on erilaisissa internetin yhteisöpalveluissa jäsenenä. Suomalaisten internetin käyttö on kohtuullisen suurta. Päivittäin internetiä käyttivät 16–74-vuotiaista vuonna 2012 78 prosenttia. Alle 45-vuotiaista lähes kaikki käyttivät internetiä päivittäin. 25–34-vuotiaista 88 prosenttia käytti nettiä useita kertoja päivässä. Suomi on internetin käytössä Euroopan kärkimaiden joukossa. Internetin käyttö kannettavalla tietokoneella ja älypuhelimella muuttuu yhä säännöllisemmäksi ja kasvaa. Vuonna 2012 kolmannes 16–74-vuotiaista suomalaisista oli internetissä ainakin kerran viikossa matkapuhelimella tai jossain muualla kuin kotona (Tilastokeskus, 2012)

Kuten jo tilastokeskuksen teettämästä tutkimuksesta selviää, niin suomalainen yhteiskunta on erittäin teknologistunut ja käyttää ahkerasti kyberavaruutta ja siellä internetiä hyväkseen. Yksityisen henkilön on siis kyettävä suojautumaan teknologistumisen aikaansaannoksen varjopuoliin eli kyberuhkiin.

Yksityishenkilön kotikoneissakin on suotavaa olla palomuuri ja tilaa säilyttävä suodattava reititin. Näiden puute saa aikaa ammottavan turva-aukon ja kokemattomankin tunkeutujan on yksinkertaisen helppoa ohittaa muut olemattomat suojausjärjestelmät (Northcutt ja Novak McLachlan 2002, 83).

Palomuuri on turvallisuusjärjestelmä, joka suojelee verkkoa muiden eri verkkojen esimerkiksi internetin käyttäjien tunkeutumiselta kotitietokoneelle. Sen tarkoitus on estää sisäisen verkon tietokoneita kommunikoimasta suoraan jonkin ulkoisen verkon tietokoneiden kanssa ja tietenkin päinvastoin. Ei pidä kuitenkaan tuudittautua siihen, että palomuuri suojaa kaikelta vaan sekin on

vain yksi keino. Väärinasennettuna tai käytettynä, se jättää suuria aukkoja mitä kautta tietokoneella päästään helposti tunkeutumaan. Yksinkertaistaen palomuuri suojaa ulkopuolisilta tunkeutujilta ja raportoi sekä pitää kirjaa havaituista tunkeutumisyrityksiltä (Hedemalm 2000, 63–64).

Internet control message protocol eli ICMP on kehitetty harmittomaksi keinoksi ilmoittaa virhetilanteista sekä vastata ja lähettää yksinkertaisia pyyntöjä. ICMP on tietokoneissa sijaitseva ohjausprotokolla, jota voidaan käyttää vääriin tarkoituksiin hyvinkin helposti. Jokaisen kotitietokoneen käyttäjän on syytä perehtyä tietokoneessaan oleviin protokolliin ja keinoihin millä saadaan luvattomat tunkeutumiset estettyä. Käyttäjän on mahdollista estää ICMP-liikenne, koska näin voidaan varmistua siitä, ettei tietokoneelle tule mitään niin sanotusti pahoja aikeita sisältyviä liikenteitä (Northcutt, ym 2002 85–105).

Tietokoneen käyttäjän mahdollisuudet havaita tietokonevirukset vaihtelevat. Osa viruksista paljastaa itsensä helposti esimerkiksi näyttämällä erilaisia ilmoituksia, soittamalla ääniä tai pahimmassa tapauksessa tyhjentämällä tietokoneen kovalevyn kokonaan. Yleisin havaitsemistapa on, kun huomataan, että jonkin ohjelman käynnistyminen kestää suhteellisen pitkään tai tietokone ei käynnisty lainkaan. Tietokoneen toiminnot hidastuvat ja kiintolevyn kapasiteetti pienenee. Mikäli tietokoneessa havaitaan tuonkaltaisia ongelmia, on käyttäjän syytä suorittaa virustentorjunta siihen mahdollisimman pian. Mikäli virustentorjuntaohjelmaa ei ole asennettuna tietokoneessa, sellainen on syytä hankkia viipymättä (Hedemalm 2000, 225).

Helpoin tapa ennaltaehkäistä saamasta saastuneita tiedostoja tietokoneella, on huolehtia tietokoneelle ajantasaisen virustentorjuntaohjelma, Mitään tiedostoja ei tule avata, jos käyttäjä ei ole varma tiedostojen puhtaudesta. Kaikki ohjelmat ja tiedonsiirtovälineet tulee tarkistaa ennen kuin ne avataan tietokoneella. Joskus, mutta onneksi valitettavan harvoin tietokone saa tartunnan huolimatta kaikista ennaltaehkäisevistä toimenpiteistä. Paniikki ei ole oikea ratkaisu vaan pitää toimia rauhallisesti ja harkiten (Hedemalm 2000, 233).

Kaikki toimenpiteet eivät onnistu ilman laajempaa perehtymistä tietokoneen käyttöjärjestelmiin ja se ei edes kuulosta kovinkaan mielenkiintoiselta. Jokaisen käyttäjän on helppo kuitenkin pitää kaikki tarvittavat päivitykset ajan tasalla mukaan lukien virustentorjuntaohjelmistot. Epäluuloisuus on aina paikallaan käytettäessä tietokonetta. Sähköpostin kautta tulleita liitetiedostoja ei koskaan tule avata, mikäli ei ole täyttä varmuutta sen sisällöstä (McClure, ym. 2002, 722).

Jokaisen tietokoneen käyttäjän on huomioita, että sitä ei voi käyttää huomaamatta internetissä. Näkyvyys ei ole riippuvainen tietokoneen suojauksista tai käyttäjästä. Tietokoneesta näkyy aina määrättyjä asioita, kun se on kytkeytyneenä internet-verkkoon. Tietokoneissa on oltava tunnistusjärjestelmä, jolla se tarvittaessa saadaan paikannettua. Tunnistusjärjestelmänä toimii IP-osoite, joka on yksilöllinen niin sanotusti tietokoneen puhelinnumero. Ilman tätä tunnistetta tietokone ei pysty vastaanottamaan mitään tietoa. Tietokoneen IP-osoite voidaan lukita kiinteäksi tai siitä voidaan tehdä vaihteleva. Lukittuna osoite on kirjautuessa verkkoon aina sama, mutta kun siitä tehdään vaihtuva niin se käyttää kirjautuessaan aina eri osoitetta. Lukittu osoite on varma maali tietoverkkorikollisille, mutta vaihtelevalla osoitteella saadaan hieman enemmän turvaa tietokoneen käyttäjälle. Pikaviestiohjelmien käyttö on yleensä aina suojaamatonta toimintaa. Ammattitaitoiset urkkijat saavat niitä halutessaan käsiinsä ja voivat lukea niitä. Tällaisia pikaviestijärjestelmiä ovat esimerkiksi messenger- ja skype-ohjelmat. Käyttäjän tulee siis harkita, mitä tietoa jakaa kyseisten viestipalveluiden kautta. Mitään arkaluontoista tai sellaista mitä ei halua ulkopuolisten tietoon ei kannata keskustella edellä mainittujen ohjelmienkautta. Luonnollisesti salasanoja tulee vaihtaa aika ajoin, koska samojen salasanojen käyttö tekee tietokoneestasi turhankin helpon saaliin (Martinez, 2013).

4.2 Yhteiskunnan suojautumiskeinot

Valtionhallinnon verkkoturvallisuus on hajautettu, jokainen hallinnonala vastaa oman alansa tietoturvallisuudesta. Vastuu on jaettu lukuisille toimijoille, joten kenelläkään ei ole kokonaiskuvaa tilanteesta. Tilanne kaipaa selkeytystä, sillä toimintaympäristön uhkakuvat lisääntyvät, joten niistä vastaavienkin pitäisi olla ajan tasalla kuinka suojaudutaan (Viestintävirasto, Signaali 2011, 18).

Yrityksen ja valtionhallinnossa työskentelevien on tärkeää suunnitella erilaiset ohjeet, mikäli haluaa turvallisuuden olevan hyvällä tasolla niin yrityksessä kuin valtionhallinnossa. Turvallisuuskäytännöt on kirjoitettava ohjeiksi, jotta jokainen tietokoneen käyttäjä näkee ne sekä voi tutustua ohjeistukseen. Riskien analysoinnin tulee olla jatkuvaa ja niihin vastaamista tulee muuttaa aina muuttuvien riskien myötä. Turvainfrastruktuurin perustaminen on aiheellista. Erilaisten ohjaustoimintojen suunnittelu ja standardit on hyvä miettiä etukäteen ja suunnitella omat jokaiselle tekniikalle mitä kyseessä oleva kulloinkin käyttää. Koska kaikki kuitenkin maksaa, tulee päättää mitkä resurssit ovat käytettävissä ja vastatoimenpiteet tulee asettaa tärkeysjärjestykseen, jotta voidaan toteuttaa edes tärkeimmät mihin on varaa. Työtä ei voi jättää tähän edellä mainittuihin

toimenpiteisiin, järjestelmää on hyvä testata aika-ajoin ja tehdä sille erilaisia tarkastuksia. Tietomurrot on havaittava ja ne tulee myös käsitellä, jotta niistä voidaan oppia sekä estää samankaltaiset tulevaisuudessa (Northcutt ym, 2002, 459).

Jokaisen tahon perussuojaukseen kuuluu, että käyttäjille on luotu omat, yksilölliset käyttäjätunnukset ja salasanat. Näillä ehkäistään sekä vähennetään sitä, että verkko ei ole kaikkien saatavilla ja käytettävissä. Käyttäjätunnuksilla voidaan myös rajata tietoja, koska jokaisen verkon käyttäjän ei ole tarpeellista päästä tutkimaan kaikkea tietomäärä mitä yrityksen tai yhteisön tietokannoista löytyy. Tämäntyyppinen järjestelmä mikä toimii käyttäjille luotujen profiilien avulla antaa korkean turvallisuustason. Näin voidaan valvoa käyttäjien saatavilla olevia resursseja (Hedemalm 2000, 41–43).

Itse verkon tietoturvallisuuttakin voidaan parantaa käyttäjätunnuksilla. Järjestelmä voidaan suunnitella siten, että se automaattisesti sulkee käyttäjän pois, joka kirjautuu virheellisesti tietokoneelle tai yrittää kirjautua väärällä tunnuksella. Palvelin voidaan myös asettaa sellaiseksi, että se ei päästä käsiksi tiedostoihin käynnistämällä järjestelmä uudelleen yrittäen näin ohittaa kirjautumisrutiini. Kaikilla tietokoneilla ei myöskään tarvitse olla levyasemia tai tallennusmahdollisuuksia. Tämä poistaa mahdollisuuden siirtää haittaohjelma epähuomiossa tietokoneelle (Hedemalm 2000, 316).

Varmuuskopiointi on myös osa suojautumista, tällä saadaan palautettua mahdollisesti kadonneita tai tuhoutuneita tiedostoja. Useimmiten informaatio on kallista ja siihen käytettyä aikaa ei saa takaisin, mikäli tietoverkkohyökkäyksen tai muun vastaavankaltaisen häiriön vuoksi menetetään arvokasta informaatiota. On muistettava varmuuskopioista se, että niillä on kaikki sama tieto mitä tietokoneillakin, mutta ei niin suojatussa muodossa. Turvallisuusnäkökulma pitää ottaa huomioon käsitellessä varmuuskopioita, koska varmuuskopiot aiheuttavat riskin järjestelmällä (Hedemalm 2000, 52–59).

Suurin riski saastuttaa tietokoneet on saada niihin tietokonevirus. Kuten tässä tutkimuksessa on jo aikaisemmin todettu, maailmassa on suuri määrä erilaisia viruksia liikenteessä joiden vaarallisuusaste vaihtelee suuresti. Markkinoilta on saatavilla erilaisia ohjelmia, joilla kyetään havaitsemaan ja poistamaan erityyppisiä viruksia. Kuitenkaan tässäkään tapauksessa täydellistä suojautumista viruksia vastaan ei ole saatavissa. Ohjelmilla voidaan kuitenkin vähintäänkin rajoittaa

virusten leviämistä. Tietokonevirusten aikaansaamaa tuhoa voidaan rajoittaa tiedostojen usein tapahtuvalla varmuuskopioinnilla, kuten tässä tutkimuksessa aikaisemmin todettiin (Hedemalm 2000, 60–61).

Koska internetin käyttö on jo arkipäivää lähes jokaisessa työpaikassa, suojautumistoimenpiteet tulee olla lähes automaattisia. Internetin turvallisuus on lähes riittämätön kaikentyyppisten tiedostojen lähettämiselle. Sähköpostin lähetykset ja muut sellaiset kannattaa tehdä harkiten tiedostojen osalta, jotka sisältävät kriittistä tietoa yrityksen tai yhteisön kannalta. Tähänkin on olemassa suojautumiskeino, nimittäin salakirjoitus. Salakirjoitus ei ole keksintönä lainkaan uusi, mutta sen käyttö sähköpostijärjestelmässä on nykyisen tietoliikenneyhteiskunnan uusi keino. Salakirjoituksen avulla saavutetaan korkea turvallisuus. Viesti muunnetaan ennen lähettämistä ja se voidaan avata luettavaksi vain tietyn avaimen avulla. Salakirjoitus voidaan jakaa kahteen ryhmään, symmetriseen ja epäsymmetriseen. Symmetrinen tarkoittaa, että salakirjoittamisen ja purkamiseen käytetään samaa avainta. Epäsymmetrinen puolestaan tarkoittaa salakirjoituksen perustuvan kahteen avaimeen. Yksityisen avaimen tuntee vain vastaanottaja, kun julkinen avain voidaan nimetä ja luovuttaa kenellä tahansa. Salaamiseen voidaan siis käyttää vain ja ainoastaan julkista avainta sekä salakirjoituksen purkamiseen vastaavaa yksityistä avainta (Hedemalm 2000, 68–69).

Tietokoneen virustartunta on syytä ilmoittaa välittömästi verkon haltijalle, jotta hän voi ryhtyä tarvittaviin toimenpiteisiin. Ilmoitus pitää tehdä myös niille henkilöille, joiden kanssa on mahdollisesti vaihtanut tallennettavilla tiedonsiirtovälineillä tietoa. Tämä tapahtuma on voinut levittää haittaohjelman heidänkin tietokoneilleen (Hedemalm 2000, 233).

Yhteiskunta on muuttunut hyvin työkeskeiseksi ja monet työtehtävistä voidaan suorittaa kotitietokoneen kautta tai työpaikan tietokoneilla, mutta omassa kotiverkossaan. Tämä toisaalta lisää riskiä joutua erilaisten kyberhyökkäyksen kohteeksi, mutta myös lisää mahdollista avunantoa. Etäkäyttöohjelmistot mahdollistavat verkon järjestelmänvalvojille ottaa tietokone hallintaansa omalta tietokoneelta (McClure ym. 2002, 576).

Yrityksen suurin tietoturvariski on kuitenkin työntekijä itse. Harvoissa tapauksissa tämä on tahallista toimintaa, vaan kyse on tietämättömyydestä tai välinpitämättömyydestä. Asioiden oikealla tiedottamisella ja kouluttamisella tämäkin ongelma saadaan hoidettua (Lagus, 2009, 8).

Puolustusvoimat, yhteiskunnan yhtenä turvallisuuselementtinä on suunnitellut yhteiskunnan suojaamista opettelemalla hyökkäämään samoilla aseilla ja keinoilla tietoverkossa, kuin yhteiskuntaa vastaan hyökätään. Puolustusvoimat on suunnitellut käyttävänsä verkkomatoja, viruksia ja haittaohjelmia. Tämä olisi yksi osa puolustusvoimien tietoverkkopuolustusta. Verkkohyökkäyskyvyn rakentamista on pidetty jotenkin liiallisena toimenpiteenä, mutta tietoturvaviranomaisen CERT-FI päällikön Erika Koivusen mukaan joissakin tapauksissa hyökkäys on paras puolustus. Puolustusvoimat on perustanut oman tietoverkkopuolustussektorin, joka omalta osaltaan edesauttaa yhteiskuntaa torjumaan erilaisia kyberhyökkäyksiä (Huhtanen 2011, HS).

Puolustusvoiminen muuttaminen hyökkääväksi tahoksi ei saavuta kuitenkaan kaikkien tahojen kannatusta, Se kuitenkin on käynyt tutkimuksessa ilmi, että kyetäkseen puolustautumaan tulee tuntea miten kybermaailmassa hyökätään. Tästä huolimatta F-Securen tutkija Jarmo Niemelä sanoi Yleisradion haastattelussa 29.10.2011, ettei suosittele vastaiskuja kyberhyökkäyksiin. Koska Stuxnet-virus aiheutti laajoja ongelmia, huolimatta siitä, että se oli räätälöity virus joka kohdistettu Iranilaiseen ydinvoimalaan (Yleisradio, uutiset).

Suomen valtio on ollut kehittämässä myös hallinnon turvallisuusverkkohanketta, jonka tarkoitus on parantaa merkittävästi tietoliikenneverkon suojaustasoa ja käytettävyyttä. Sen avulla saadaan turvattua kriittisen tiedon eheys, luottamuksellisuus ja tiedon saatavuus eri olosuhteissa. Verkkohankkeen avulla tietoturvallisuus on tarkoitus varmistaa tehokkaalla valvonnalla ja salaamisella. Turvallisuusverkko hankkeen tarkoitus on turvata johtaminen kaikissa olosuhteissa. Kyseinen hanke on valtioneuvoston ja turvallisuusviranomaisten korkean varautumisen ratkaisu. Kyseinen turvallisuusverkko hyödyntää jo olemassa olevan tietoverkon ja olemassa olevat palvelut niin pitkälle kuin mahdollista. Verkko on tarkoitus suorittaa viiden hallinnonalan yhteistyönä. Yhteistyöosapuolina toimivat valtionvarainministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö sekä ulkoministeriö (Valtionvarainministeriö, 2011, 2, 5, 10).

Yksi keino yhteiskunnalle on puolustautua kyberuhkilta ja niiden aiheuttamilta häiriöiltä lainsäädännön avulla. Suomen lakeja on muutettu, mutta tuomiot tietoverkkorikollisuudesta eivät ole vielä samalla tasolla kuin ulkomailla. Esimerkiksi Britanniassa tuomittiin kolme niin sanottua nettiterroristia vankeuteen, syynä oli terrorismiin yllyttäminen verkon kautta. Miehet olivat tehneet yhteistyötä Al-Qaidan kanssa ja verkkosivuillaan yllyttäneet surmaamaan ei – muslimeja. He olivat perustaneet verkkosivustoja käyttäen varastettujen luottokorttien henkilötietoja (Taloussanomat 8.7.2007).

Edellä mainitussa esimerkissä, nettirikolliset olivat varastaneet luottokortteja ja hyödyntäneet niiden henkilötietoja. Tämä niin kutsuttu identiteettivarkaus on valitettavan yleistä ja siihen on keskittynyt kokonainen laiton toimiala, jonka tehtävänä on suorittaa henkilötietojen varastamisia ja myydä näitä saatuja tietoja eteenpäin toisille varkaille internetin kautta (Norton, 2013). Identiteettivarkaudet ovat ongelma yhteiskunnalle kuin myös luonnollisesti yksityiskäyttäjälle.

Kyberturvallisuus on iso ja kannattavaa liiketoimintaa. Kyberturvallisuuden tarpeellisuudesta ei ole vara tinkiä. Esimerkiksi maailmanlaajuisesti kyberturvallisuuteen käytettiin vuonna 2011 60 biljoonaa dollaria (Pricewaterhousecoopers, 2011, 4)

5. AINEISTON KESKEISIÄ TEEMOJA

Aineiston kerääminen tutkimukseen oli suhteellisen haastavaa. Haasteelliseksi sen teki tutkimuksessa käytetyn aineiston englanninkielisten materiaalien runsaus. Kyberuhkista on laadittu useita erilaisia lehtiartikkeleita ja tutkimuksia, jotka käsittelevät kyberiä sen eri näkökulmista. Julkaistua kirjallisuuttakin kyberistä on olemassa runsaasti, toki vain englanninkielisenä. Tutkimus rajattiin koskemaan yhteiskunnan toimintaa uusien uhkien kanssa ja uusista uhkista tässä tutkimuksessa käsitellään vain kyberuhkaa. Vanhat olemassa olevat uhkat ja niiden määritelmät jätettiin rajauksessa tämän tutkimuksen ulkopuolelle, kuitenkin ne ovat olleet taustoittamassa tutkimuksen varsinaista aineiston analyysia. Tekstien tarkka tulkinta ja teksteistä yhtäläisyyksien sekä erojen etsintä nosti esiin näkökulmia, joita oli syytä tarkastella tarkemmin. Kyberstrategiassa ja muissa kyberturvallisuutta käsittelevissä teksteissä toistui tiettyjä samoja teemoja, jotka valittiin tarkempaan analyysiin.

5.1 Kyberturvallisuuden lainsäädäntö

Lainsäädännölliset asiat nousevat keskeisesti esiin kerätystä aineistosta. Kyberstrategiassa onkin keskeistä puhua lainsäädännöstä, koska se sanelee kansallisesti ja kansainvälisesti toimintaraamit missä eri viranomaiset ja muut vastaavat toimijat voivat työskennellä. Lainsäädäntö ei kuitenkaan ole vielä ajan tasalla kaikissa kyberasioissa Suomessa kuin ei myöskään kansainvälisesti ja olemassa olevat lait eivät ole kattavia.

Tulevaisuudessa Suomeen perustettava kyberturvallisuusvirasto rakennetaan CERT-FI luomalle pohjalle. Virastosta tulee kyberasioita valvova ja organisoiva virasto, joka koordinoi kaikkea kyberturvallisuuteen liittyviä asioita. Huolimatta siitä, että kyber ei ole toimintaympäristönä mikään uusi elementti, sen olemassaoloon on herätty suhteellisen myöhään. Myöhäiseen heräämiseen toki vaikuttaa tietotekninen kehitys ja globalisaation yleistyminen. Kyberavaruudessa on pitkään voinut toimia lähes mielivaltaisesti, ilman pelkoa rangaistuksesta ennen kuin siihen on puututtu. Miten siihen on puututtu tai tulevaisuudessa pystytään puuttumaan, niin tämä on toinen juttu.

Kyberista tai kyberturvallisuudesta on jo sanana itsestään tullut jonkin asteinen muoti-ilmiö, josta puhutaan lähes päivittäin eri medioissa. Asia on vakava ja siihen tuleekin ottaa kantaa. Tehokkain ja ehkä ainoa asia millä siihen saadaan otettua kantaa sulkematta virtaa tietokoneista tai tietover-

koista on lainsäädäntö. Lainsäädäntöä tulee jatkuvasti kehittää ja pitää ajan tasalla tietoyhteiskunnan kehittyessä. Lainsäädännöllä yhteiskunta luo rajoja, joita kansalaiset noudattavat. Kuten tutkimuksesta on käynyt ilmi, rajojen noudattaminen on joillekin hankalaa. Rikolliset eivät kunnioita lakeja ja aikaansaavat näin vahinkoa. Lainsäädännön tehokkuudella tarkoitankin sen tuomia rangaistusmahdollisuuksia joita rikolliselle voidaan langettaa heidän jäätyään kiinni rikoksesta.

Huoltovarmuuslaki (HE 44/2005 vp.) luo pohjan ja kokonaiskäsityksen yhteiskunnan turvallisuuden käsittelylle. Suomessa huoltovarmuus perustuu julkisen vallan ja elinkeinoelämän yhteistyöhön. Sen keskeisiä perusteita on toimiva hallinto ja julkinen palveluntuotanto, kyllin vakaa rahoitusasema julkisella sektorilla, tasapainoinen rahoitussektori yleensä ja julkinen palvelutuotanto sekä kansalaisten käytössä oleva ostovoima. Laissa käsitellään kriittisten järjestelmien suojaamista, mutta huoltovarmuuslaki jättää kuitenkin vielä aukkoja miten kriittisiä järjestelmiä yksilöidään (Aine, Nurmi, Ossa, Penttilä, Salmi, Virtanen 2011, 109).

Tässä tutkimuksessa on käsitelty kyberia uhkana, joka on vasta viime vuosina huomioitu uhkaksi siinä missä suoranainen hyökkäys Suomea kohtaan on ollut aina uhka. Fyysistä uhkaa meillä on torjumassa puolustusvoimat, jonka tehtävät on määritelty laissa.

Laki puolustusvoimista, 11.5.2007/551 (Oikeusministeriö 2007) säätää puolustusvoimien tehtävät, toimivallan ja organisaation. Laissa puolustusvoimille on määrätty tehtäväksi muun muassa Suomen sotilaallinen puolustaminen. Kyseinen laki ei ole ollut voimassa kovinkaan montaa vuotta ja siinä on hieman otettu kantaa puolustusvoimien tehtäväkentän laajentamiseen. Uudistettu laki rinnastaa aseellisen hyökkäyksen kanssa samaan sitä vastaavan ulkoisen uhan. Ulkoisella uhalla tässä tapauksessa voidaan ymmärtää kyberuhka, joka tulee meille tietoverkkoja pitkin (Aine, ym. 2011, 67–68).

Laki kuitenkin rajoittaa toimivaltuuksia, koska kansainväliset säädökset antavat kehyksen mitä myös pitää noudattaa. Kyberia vastaan on vaikea toimia pelkästään sotilaan henkilökohtaisella aseella tai vaikka tykistön iskulla. Tutkimusta tehtäessä oli havaittavissa muissakin maissa tämä sama lainsäädännöllinen ongelma kuin meillä Suomessa. Lakien muuttaminen ei tapahdu kädenkäänteessä ja näin muutos tulee valitettavasti huomattavasti jälkijunassa kuin asioiden teknologinen kehitys. Kuitenkin useissa valtioissa kyberiskut rinnastetaan selkeästi fyysiseen iskuun eli

samalle tasolle kuin suoranainen ohjusisku. Joissakin valtioissa tämä on johtanut siihen, että se antaa valtion asevoimille mahdollisuuden vastata kyberiskuun sotilaallisesti eli käyttää vastaamiseen suorastaan raakaa asevoimaa.

Pitääkö meidän ohjata puolustusvoimia tähän samaan suuntaan vai onko parempi pitäytyä edelleen jäykän torjuvana ja kehittää muita keinoja vastata kyberin tuomiin uhkiin tai ongelmiin? Voimmeko kehittää vastatoimeksi niin sanottuja kyberaseita? Vastaisimme tietoverkkohyökkäykseen samankaltaisella aseella kuin meitä vastaan käytettiin. Asejärjestelmätkin ovat viime vuosina teknistyneet runsaasti. Tällä hetkellä jopa tykin tuliasemassa on nähtävissä kannettavia tietokoneita, modeemikaapeleita ja jopa reitittimiä. Tämä muuttaa sodankuvaa jopa varusmiestasolla vastaamaan osin nykyaikaista sodankäyntiä. Olemmeko kuitenkin menossa kohti kyberarmeijaa vai ainoastaan hyödyntämässä teknologiaa mielestäni järkevällä tavalla. Tämä teknologistuminen madaltaa kynnystä ainakin mielikuvitukselle, jossa puolustusvoimat taistelee jossain vaiheessa kybersodankäynnin mahdollistamilla keinoilla. Tätä ei ole kuitenkaan vielä linjattu vaan ajatus on ihan tutkijan omaa lennokasta mielikuvitusta. Toisaalta se vaatisi hyvin laajan lakimuutoksen ja kenties se muuttaisi meidän puolustusvoimamme hyökkäysvoimaksi ja se ei ole välttämättä haluttu suunta.

Lakeja on kuitenkin hieman jo ehditty saattamaan vastaamaan nykypäivän ongelmia. Valmiuslaki 29.12.2011/1552 (Oikeusministeriö 2011) määrittelee yhteiskuntaa koskevia poikkeusoloja. Kyseisessä laissa on määritelty selkeästi muutostilat, jotka voivat ravistella yhteiskuntaamme. Poikkeusolona pidetään aseellista tai siihen rinnastettavaa hyökkäystä tai sen jälkitilaa. Tällainen poikkeustilan torjuminen vaatii lain mukaisten toimivaltuuksien käyttöönottoa. Uudistus antaa viranomaisille ja puolustusvoimille mahdollisuuden puolustautua kybertoimintaympäristössä. Viranomaiset saavat tämän lain puitteissa enemmän valtuuksia, kuten vaikkapa katkaista tietoverkkoyhteydet ulkomaille tai kenties avata joitain yhteyksiä lisää. Tämänkaltaisesta lakiasetuksesta on jo enemmän konkreettista hyötyä, koska se antaa mahdollisuuden toimia fyysisesti sellaista uhkaa vastaan mikä ei edes vaikuta uhkalta. Monet niin sanotusti normaalit asiaan perehtymättömät kansalaiset eivät osaa kokea kyberuhkaa varsinaisena uhkana. Syy tähän on todennäköisesti se, ettei kyberuhka suoranaisesti kosketa jokaisen yhteiskunnan jäsenen arkea. Kaikkia yhteiskuntamme jäseniä ei kiinnosta tietoverkkohyökkäykset tai sellaisen hyökkäyksen johdosta jumiin menneet ministeriön internet-sivustot (Turvallisuus ja puolustusasiain komitea 2012, 10).

Kuten tutkimuksesta on käynyt ilmi, niin vastaavanlainen tietoverkkohyökkäys internetsivusto- ja vastaan on vain murto-osa siitä todellisuudesta, minkä kyber mahdollistaa rikollisille tai muille rikollisen kaltaisille toimijoille. Tietoverkkohyökkäyksiä vastaan voidaan toimia kaikkialla missä on tietokone ja tietoliikenneyhteydet. Eihän hyökkäyksen ole pakko kohdistua minnekään valtionhallinnon virastoihin tai muihin vastaaviin. Hyökkäys voi kohdistua pankkeihin, sähkölaitoksiin, lähestulkoon minne tahansa. Onneksi tähän on pyritty ottamaan kantaa lainsäädännöllä. Lakien tarkoitus on kuitenkin suojella tai turvata jonkin ihmisryhmän tai asioiden etu.

Suomen rikoslain 34 luvun 9 a §:n 11.5.2007/540 mukaan vaaran aiheuttaminen tietojenkäsittelylle on rangaistava teko. Tällä rikoslain pykälällä yhteiskunta voi ottaa kantaa ja rangaista esimerkiksi hakkereita tai muita tietoverkkorikollisia. Sen avulla henkilö, joka aiheuttaa haittaa tai vaaraa tietojenkäsittelylle tai tieto- ja viestijärjestelmien turvallisuudelle voidaan asettaa syytteeseen ja myöhemmin jopa tuomita tällaisesta rikkomuksesta. Tällä hetkellä mikään laki ei kuitenkaan rankaise tietokonevirusten laatimisesta. Tekeminen ei ole rikollista toimintaa, ainoastaan tietokoneviruksen saattaminen levitykseen muuttaa teon rangaistavaksi (Oikeusministeriö 2007).

Lainsäädäntöä pyritään kokoajan kehittämään vastaamaan muuttunutta ja yhä edelleen muuttuvaa yhteiskuntaa. Etenkin sitä pyritään kehittämään vastaamaan yhteiskuntaa uhkaavia tekijöitä kohtaan, kuten sellaisia uhkia tai toimia mitä toiminta kyberissä voi aiheuttaa. Lainsäädännölliset keskustelut kyberin ympärillä ovat siis tarpeen ja erittäin ajankohtaisia. Tarpeellisuutta korostaa etenkin Suomen kansallisessa kyberstrategiassa esitetty visio, että Suomi olisi vuonna 2016 johtava valtio kyberasioissa. Mahdollisen vision toteutuminen vaatii siis edelläkävijän roolia myös lainsäädännön osalta.

Vision toteutuminen ei ole pelkästään Suomen lainsäädännöstä riippuvainen. Kyberuhka on globaali, valtion rajoja kunnioittamaton. Uhka, mikä ei kunnioita valtion rajoja tai kyseisen valtion lainsäädäntöä on vaikea pysäyttää. Tämä vaatii kansainvälistä yhteistyötä, jotta saadaan muodostettua lainsäädännöstä sellainen verkosto, jolla pystytään asettamaan vastuuseen rikolliset, haittaa tekevät tahot. Kansallisten ja kansainvälisten lakien tulee olla rajoja ylittävät ja niiden käytettävyys pitää hyväksyä globaalilla tasolla, jotta saavutettaisiin lainsäädännöllisesti toimiva, pitävä kokonaisuus.

5.2 Kyberturvallisuuskeskuksen merkitys kansallisesti

Tutkimusta tehtäessä on aineistosta noussut monella tapaa esiin kyberavaruuden monimuotoisuus ja mitä kaikkea ongelmia sen avulla voidaan yhteiskunnalle aiheuttaa. Kyberavaruus ei itsessään ole ongelma vaan se on väline. Tahot, mitkä käyttävät kyberavaruutta rikollisessa hyötymistarkoituksessa muodostavat ongelman tehdessään kyberavaruuden mahdollisuuksista aseen.

Kyberavaruus ja sen kautta ilmenneitä ongelmia sekä mahdollisuuksia on syytä tutkia tarkemmin. Tutkimiseen ja asioiden kehittämiseen on todellista tarvetta, sillä Suomeenkin kohdistuu päivittäin eriasteisia tietoverkkohyökkäyksiä. Tähän tarpeeseen on laadittu Suomen kyberturvallisuusstrategia. Kyberturvallisuusstrategiassa otetaan kantaa kehitys ja tutkimustyöhön. Suomeen ollaan perustamassa kyberturvallisuuskeskusta. Kyberturvallisuuskeskuksen tarkoitus on koordinoida ja tutkia kaikkia kyberturvallisuuteen liittyviä asioita. Keskuksen tehtävänä on ottaa selvää kyberturvallisuusasioista kaikista mahdollisista lähteistä ja jakaa sitä kaikille toimijoille, jotka voivat arvioida kyberturvallisuuden aiheuttamia häiriöitä omaan toimintaansa liittyen (Suomen kyberturvallisuusstrategian taustamuistio 2013, 10).

Kuten tutkimuksesta käy ilmi, kyberuhkat kehittyvät erittäin nopeasti ja muuttavat muotoaan. Tämä asettaa suuren haasteen asioiden tutkimiselle ja kehitystyölle. Kehitystyö onkin yksi keskeisimmistä ennaltaehkäisyn keinoista taistella kyberturvallisuuden uhkia vastaan. Tutkimuksen lähdeaineistossa, lähes jokaisessa painotettiin kansainvälisen yhteistyön merkitystä ja tutkimustyötä. Kansainvälisellä yhteistyöllä on suuri merkitys tutkimukseen ja kehitykseenkin. Tiedon jakaminen puolin ja toisin kehittää valtioista parempia vastaamaan kyberuhkiin.

Suomessa on poikkeuksellisen erinomainen tilanne, kun valtiohallinnon ja yritysten edustajat tekevät paljon yhteistyötä kyberturvallisuuden eteen. Kyberturvallisuuden tutkimus ja kehitys eivät ole yksinomaan yhteiskunnan poliittisen johdon tehtävä. Yhteiskunnan ei ole mahdollista vastata yritysmaailmassa syntyneisiin kyberturvallisuuden paineisiin yksin, vaan yritysten on tehtävä yhteistyötä valtiohallinnon edustajien kanssa. Kyberturvallisuuskeskus pyrkii tähän samaan tavoitteeseen. Monipuolinen osaaminen kyberturvallisuuskeskuksessa takaa sen, että tietoturvapoikkeamien ja niiden ratkaiseminen palvelee kaikkia yhteiskunnan jäseniä. Tietoturvakeskuksen lisäksi GovCERT, joka on kymmenen eurooppalaisen tietoturvaviranomaisen muodostama yhteistyöverkosto (Viestintävirasto, Signaali 2011, 18). Yhdessä virastot tekevät työtä paljastaakseen

julkiseen hallintoon kohdistuvia tietoturvaloukkauksia (Suomen kyberturvallisuusstrategian taustamuistio 2013, 10).

Kyberturvallisuuden hallinta koostuu monista osa-alueista kuten itse kyberturvallisuuskin. Yli puolet kapasiteetista käytetään koulutukseen ja tutkimustyöhön. Tietoturvahyökkäyksien havaitsemiseen ja niistä tiedottaminen lohkaisee pienen osan kyberturvallisuuden hallinnasta. Tiedottaminen on tärkeä osa tässä kokonaisuudessa. Tiedon jakamisella voidaan kenties välttyä samalta ongelmalta uudelleen ja etenkin tiedottamisella kansainvälisesti voidaan ennaltaehkäistä monia vastaavia tapahtumia (Suomen kyberturvallisuusstrategian taustamuistio 2013, 11).

Ongelmien havaitsemisesta seuraa luonnollisesti ongelman rajoittaminen. Nopealla rajoittamisella saadaan ongelman leviäminen toivottavasti estettyä tai käynnistettyä mahdollisia vastatoimenpiteitä. Ongelman ilmestyessä se todennäköisesti ehtii tehdä jonkinasteisia tuhoja, joista yhteiskunnan pitää selvitä. Palautuminen, pääseminen normaalitilaan onkin osa kokonaisuutta. Toipuminen on oma prosessinsa, joka pitää myös hallita. Kaikkea tätä kyberturvallisuuskeskuksen onkin tarkoitus koordinoida ja valvoa. On hyvä asia yhteiskunnalle, että meille tulee yksi paikka mihin keskitetään osaamista ja mistä osaaminen on kaikkien ulottuvilla.

Kyberturvallisuuskeskus hoitaa vuoropuhelua eri toimijoiden kanssa ja luo suhteita uusiin tarvittaviin yhteyksiin. Keskus palvelee yhteiskunnan lisäksi yritysmaailmaakin, toki onhan yritysmaailma ja kaupankäynti merkittävä osa yhteiskuntaa. Keskuksella on kaikki ovet vielä avoinna, kun sen suuntaa ei ole vielä tarkkaan määritelty. Kyberturvallisuuskeskuksesta on tarkoitus laatia puolueeton ja neutraali virasto, joka ei ole poliisin tai puolustusvoiminenkaan alaisuudessa. Keskuksen on tarkoitus palvella kaikkia instansseja kansallisesti ja kansainvälisesti. Kansainvälisyyteen tulee todennäköisesti panostaa enemmän, koska kyberturvallisuus on kansainvälinen asia (Suomen kyberturvallisuusstrategian taustamuistio 2013, 11).

Kuten tutkimuksessa on todettu, tietoyhteiskunta on maailmanlaajuinen ja tiedonsiirto maapallon eri kolkista tapahtuu välittömästi. Samalla nopeudella leviävät kyberavaruudessa niin hyvät kuin huonotkin bitit.

Kyberturvallisuuskeskuksen täyttä osaamista ei vielä tiedetä, koska sen syntyhistoria on vasta alkamassa. Se jää nähtäväksi, että onnistuuko keskus auttamaan Suomea tavoittamaan visionsa

ollakseen kärkimaa kyberturvallisuusasioissa. Keskus tarvitsee toimiakseen tietoturva-asiantuntijoiden täyden tuen ja heidän ajan tasalla olevan ammattitaitonsa. Tämä ei onnistu ilman nykyisten tietoturva-asiantuntijoiden yhteistä panostusta ja innovatiivisuutta. Kyberturvallisuuden häiriöitä ei ratkaista irrottamalla internet-modeemi tietokoneen kyljestä, kaikki me pystymme siihen. Ongelma tulee olla ratkaistu ennen kuin ongelmaa on edes syntynyt.

5.3 Kyberturvallisuus

Jokaisessa tutkimuksessa käytetyssä lähteessä nousi esiin kyberturvallisuus. Se on selkeästi keskeisin osa-alue puhuttaessa kyberasioista lainkaan. Ensin määritellään kyber ja sitten millainen se on toimintaympäristönä. Kyberympäristöstä ei voi puhua ellei puhu kyberturvallisuudesta, koska digitaalinen ympäristö aiheuttaa tietynlaista turvattomuutta ja uhkaa. Kyberturvallisuus on tullut entistä enemmän tärkeäksi ja merkityksekkäämmäksi asiaksi, sillä lähestulkoon kaikki toiminta tapahtuu tietoliikenneverkoissa (Suomen kyberturvallisuusstrategia, 2013, 5).

Yhteiskunnan muuttuminen teknologisempaan suuntaan on muuttanut väistämättä turvallisuusnäkemystä. Tämän tutkimuksen rajaus, kyberuhka yhteiskunnan uutena uhkana johdattaa tähän kyberturvallisuuteen. Mikäli jokin asia aiheuttaa uhkaa, niin sille pitää vastapainona löytyä turvallisuutta ja rauhaa. Ei siis ole mikään ihme, että kyberturvallisuus on esillä alan keskeisimmissä lähteissä ja päivittäisessä mediassakin.

Kyberturvallisuus koskettaa meitä jokaista yhteiskunnan jäsentä. Kyberturvallisuudesta puhuminen pitääkin saattaa jokaisen kansalaisen kuultavaksi, koska sen häiriötilat heijastuvat konkreettisesti myös yksilötasolle. Kyseessä ei siis ole olomuoto, joka koskettaisi pelkästään valtion poliittista johtoa tai yritysmaailmaa.

Uudessa kyberturvallisuusstrategiassa todetaan kyberturvallisuuden perustuvan yhteiskunnan tietojärjestelyihin. Sen edellytyksenä on tarkoituksenmukaiset ja riittävät tietojärjestelmien turvallisuusratkaisut. Yksityishenkilönkin on syytä olla perillä mahdollisista suojauskeinoista miten voi toimia kyberturvallisuutta parantaen. Rikollisten toiminta kohdistuu normaalin käyttäjään siinä missä valtiolliseenkin tasoon. Rikollinen uhkaa turvallisuutta hyötymistarkoituksessa, joten kaikki me kaikki olemme potentiaalisia uhkia. Voisi kuvitella, että yksittäinen kansalainen ei ole mitenkään arvokas kohde rikolliselle, mutta kun kansalaisia on monia, niin se tekee rikoksesta kan-

nattavan. Tällä tarkoitetaan sitä, että monet tietokoneen käyttäjistä ovat aika huolimattomia suojausten suhteen. Salasanat ovat helposti selvitettävissä, virusten torjuntaohjelmat eivät ole ajan tasalla ja niin edelleen. Tällaiseen kohteeseen, kun rikolliset pääsevät iskemään lukuisia kertoja se on jo taloudellisesti kannattava toimenpide. Kotitietokoneen käyttäjällä on valitettavan usein illuusio turvallisuudesta. Tietokoneen käyttäjät uskottelevat ettei tähän tietokoneeseen mikään iske. Tietoverkkorikosten seurauksena henkilökohtaisia tietoja voidaan vuotaa internetin keskustelupalstoille tai jonnekin muualle nähtäväksi. Tämänkaltainen toiminta voi saada siis laajempaa tuhoa kuin pelkästään salasanojen selvittäminen.

Valtionjohto ja yritysmaailma eivät voi tuudittautua ajatukseen, että mitään ei tapahdu yhteiskunnalle, kuten ei myöskään yksittäiselle kansalaiselle. Kyberturvallisuus ei ole pelkästään tietoverkoissa tapahtuvaa haitantekoa vaan se voi levitä sieltä ja aikaansaada tuhoa tai ongelmia yhteiskunnan elintärkeille toiminnoille. Kyberstrategia on osa yhteiskunnan elintärkeiden toimintojen strategiaa ja siinä otetaan kantaa myös tähän edellä mainittuun vaaratilanteeseen (Suomen kyberturvallisuusstrategia 2013, 8).

Turvallisuusajatus pitää iskostaa alimmalta tasolta aina johtoon asti. Ongelmaksi tällaisen kyberturvallisuuden saavuttamiseksi muodostaa raha, kyberturvallisuudella rahastetaan ja se on iso kaupallinen tekijä. Laki ei velvoita suojautumaan kyberturvallisuuden häiriöiltä. Sellaista lakia on vaikea edes valmistella tai saattaa voimaan, joka pakottaisi kansalaisen maksamaan omasta turvallisuudestaan. Turvallisuuden saavuttaminen on jokaisen henkilön oma asia, kaikki eivät edes välttämättä koe kyberuhkaa minään turvallisuusongelmana niin miksi sellaisia henkilöitä kiinnostaisikaan kyberturvallisuuden tila. Valtionhallinnon tulee tehdä töitä sen eteen, että saamme kyberturvallisuuden merkityksen nostettua jokaisen kansalaisen tajuntaan. Kyberturvallisuuden eteen vaaditaan kaikkien työ, sillä se on kokonaisuus mikä koskettaa kaikkia. Tieto on sellainen pääoma, jota meidän tulee ymmärtää suojata.

Ensimmäiseksi kaikki ovat valmiina suojaamaan omat taloudelliset resurssit ja kaikki muu jää sen ulkopuolelle. Tähän ajattelumalliin on saatava muutos, se voidaan toteuttaa suurimmaksi osin asennekasvatuksella. Viranomaisten tuleekin panostaa yhteistyöhön eri ryhmittymien välillä, jotka toimivat kyberympäristössä. Ensimmäinen askel tähän taitaa olla otettu, kun Suomeen perustetaan kyberturvallisuuskeskus, joka tulevaisuudessa koordinoi kaikkea kyberiin liittyvää. Kyber-

turvallisuuskeskus tulee olemaan avainasemassa tämänkaltaisessa kasvatustyössä (Suomen kyberturvallisuusstrategia 2013, 7).

Kyberturvallisuuskeskuksen suurin työ on saada ihmiset ymmärtämään käyttäytymään kyberympäristössä oikealla tavalla. Siellä pitääkin olla samat pelisäännöt kuin virtuaalimaailman ulkopuolella. Omalla käytöksellä ratkaistaan paljon. Pitää harkiten paljastaa itsestään virtuaalimaailmassa, kaiken minkä sinne itsestään antaa niin sinne myös jää. Tällä tarkoitetaan valokuvia, tekstejä ja niin edelleen. Se ei riitä, että ne poistetaan joltain sivustolta vaan tieto todennäköisesti jää jonnekin palvelimen muistiin vielä pitkäksi aikaa poistamisen jälkeenkin

Kyberturvallisuus pitää nähdä myös toisinpäin. Suomen korkeassa visiossa maamme on kyberasioiden kärkivaltio vuonna 2016, joten voidaan nähdä kyberturvallisuuden häiriötilanteet mahdollisuutena. Kyberturvallisuus on asia, josta ollaan valmiita maksamaan niin me voimme kehittää Suomen yhteiskuntaa puolustamaan sitä vastaan ja saaden tästä osaamisesta myyntivaltin itsellemme (Suomen kyberturvallisuusstrategia 2013, 3).

Suomessa tätä tarvittavaa tietoteknistä osaamista ja yhteistyötä eri instanssien väliltä löytyy. Nyt tarvitsee luoda vain kyberturvallisuuteen sellainen tuote, joka ensisijaisesti suojaa Suomen yhteiskunnan toiminnot ja sen jälkeen sitä voi hyödyntää maamme etuihin kansainvälisesti. Onko etuina sitten taloudellinen hyöty vai maineen kasvattaminen niin se on taas toinen juttu.

5.4 Häiriötilanteiden jälkeinen palautuminen

Useassa tutkimuksessa käytetyssä aineistossa puhuttiin häiriötilanteista ja kuinka niistä palaudutaan. Kyberturvallisuuden tullessa uhatuksi ja joutuessa häiriötilaan, on järjestelmä saatava palautettua ennen häiriötilaa olevaan olotilaan. Ainahan tämä ei ole mahdollista, mutta järjestelmät pyritään saattamaan lähes ennalleen. Tämä sama tilanne koskee niin yksityishenkilöä kuin valtion hallintoakin. Lähtökohtana on, että kyberturvallisuuden sietokyvyn on oltava suuri, koska tiedonsiirtoverkoissa tapahtuu kyberhyökkäyksiä päivittäin (Valtionvarainministeriö ICT, 2012, 21)

Huolimatta kaikesta panostuksesta, mitä kyberturvallisuuteen on sijoitettu, suojausjärjestelmät onnistutaan toisinaan läpäisemään. Tietomurtojen tekijät onnistuvat valitettavankin usein. Onnistuminen on toisinaan kiinni käyttäjän huolimattomuudesta tai järjestelmään ilmenneistä vioista. Järjestelmä koostuu kuitenkin tietokoneiden välisestä verkosta ja toiminta on riippuvainen teknologiasta. Toisinaan vain jokin järjestelmän osa voi pettää ja tämä saa aikaan heikkouden jota tietoverkkorikolliset pääsevät hyödyntämään murtautuen järjestelmään.
Järjestelmästä palautumisen toimenpiteet koskevat niin yksityishenkilöitä kuin muitakin toimijoita. Otetuilla varmuuskopioilla taataan, että kaikkea tietoa ei menetetä vaan siitä on olemassa aina kopio jossain erillisessä paikassa tallessa. Näiden kopioiden avulla voidaan palauttaa järjestelmä tilaan, jossa se oli ennen toimintahäiriötä (Hedemalm 2000, 52).

Välttämättä palautuminen ei ole niin yksinkertaista, koska toisinaan vian etsiminen järjestelmästä voi kestää. Ammattitaitoiset hakkerit kykenevät soluttamaan tiedostaja siten, että jopa asiantuntijalta voi kestää niiden löytäminen ja poistaminen. Yritysten ja muidenkin tahojen toiminta kyberhyökkäyksiä vastaan pitää olla ripeää. Nopea toiminta edesauttaa palautumista, koska järjestelmä ei ehdi kokea niin suurta tuhoa. Hidas reagointi kostautuu taloudellisina tappioina ja pahimmillaan voi kaataa yrityksen, jos jotain liikesalaisuuksia pääsee vuotamaan väärille tahoille (Hedemalm 2000, 225).

Tutkimuksesta käy ilmi, että palautuminen on yhteiskunnankin etu. Yhteiskunnan elintärkeiden toimintojen ylläpitäminen vaarantuu, mikäli järjestelmiin tunkeutumista ei saada pysäytettyä tai havaittua ongelmaa poistettua. Viranomaisilla on oltava tarpeeksi laajat toimivaltuudet, resurssit sekä valtion hallinnon tuki, jotta palautuminen olisi nopeaa ja sujuvaa.
Tähänkin avuntarpeeseen on vastaamassa tulevaisuudessa kyberturvallisuuskeskus, jonka koordinoinnin avulla tietoturvauhkat saadaan torjuttua nopeasti ja varmasti. Mikäli jokin taho joutuu kyberhyökkäyksen kohteeksi ja uhriksi niin salailu on huono vaihtoehto. Tässä asiassa avoimuus ja tiedottaminen kannattavat, koska näin saadaan valistusta muille käyttäjille. Mahdollisten hyökkäysten leviäminen saadaan estettyä tai ainakin hidastettua. Tiedottaminen sekä varoittaminen siis nopeuttavat palautumista ja ovat mielestäni yksi helpoimmin suoritettavista palautumisprosessin nopeuttajista. Mikäli hyökkäys on tehnyt enemmän tuhoja, kuten katkaissut vaikka vedenpuhdistamoilta pumppaamojen toiminnat tai jotain muuta sellaista, on puolustusvoimat valmiina antamaan virka-apua sitä tarvitseville. Palautuminen ei siis välttämättä ole pelkästään tietokoneiden kautta suoritettavaa vaan se voi olla konkreettista fyysistä apua (Suomen kyberturvallisuusstrategian taustamuistio, 2013, 11).

Palautuminen ei koske pelkästään tietokoneita vaan palautuminen on myös osa oppimisprosessia, jota tietokoneen käyttäjä joutuu käymään läpi. Mikäli jälkeenpäin käytävä palautuminen jää puoliväliin tai sitä ei suoriteta lainkaan, voi tietokoneen käyttäjälle jäädä häiritsevä epävarmuus toimia enää tietokoneella. Palautuminen tulee siis suorittaa kokonaisvaltaisesti ensin järjestelmälle ja sitten järjestelmän käyttäjälle.

6. POHDINTA

Kokonaisuutta katsoen tutkimuksen tekeminen oli mielenkiintoista ja antoisaa, juuri aihevalinnan ansioista. Mielenkiintoisemman kirjoittamisesta teki asian ajankohtaisuus sekä median tuoma julkisuus. Mikäli aika ja resurssit olisivat antaneet myöten, tutkimuksessa olisi voinut keskittyä myös tekniseen puoleen.

Tässä tutkimuksessa on hyödynnettyjä lähteitä 82 kappaletta. Lähteinä käytettiin kirjallisia ja sähköisiä sekä muita lähteitä. Moni kirjallisista lähteistä oli valtavan laajoja, joissa sivumäärä oli suuri. Näistä lähteistä tutkimuksessa etsittiin vain tutkimuksen kannalta keskeisimmät asiat. Tutkimuksessa käytettiin lähteinä myös useita englannin kielellä kirjoitettuja julkaisuja, joka lisäsi tutkimuksen tekemisen monipuolisuutta ja haastavuutta.

Tutkimuksen tavoitteena oli avata lukijalle yhteiskuntaa vaanivia uhkia ja miten niiltä suojaudutaan. Tutkimuksen aikataulutuksen vuoksi tässä työssä keskityttiin vain kyberuhkaan. Kyberuhka osoittautui laajemmaksi kokonaisuudeksi, kuin ennen tutkimuksen aloittamista ajattelinkaan. Tutkimusmetodeihin tutustumalla todettiin, että tälle tutkimukselle sopiva tutkimusmenetelmä oli laadullinen tutkimus ja teoriaohjaava sisällönanalyysi. Valitsemalla teoriaohjaavan sisällönanalyysin sain selkeytettyä ajatuksen miten tutkimus tehdään ja miten se viedään sujuvasti päätökseen.

Ensimmäiseksi tutkimusta aloittaessa oli perehdyttävä taustoihin ja aikaisempiin aiheesta tehtyihin tutkimuksiin sekä julkaistuihin materiaaleihin. Tutkimuksen alussa määriteltiin ja selkeytettiin myös tärkeät tutkimukseen liittyvät käsitteet. Toisessa vaiheessa perehdyttiin itse kyberiin, uutena yhteiskuntaa uhkaavana tekijänä. Tutkimuksessa käytiin läpi myös millaista erilaista toimintaa kyberissä oikein on. Lisäksi perehdyttiin kyberuhkan tuomiin ja herättämiin psykologisiin vaikutuksiin. Siihen miten nykyaikainen tietoliikenneyhteiskunta herättää käyttäjissä pelkoa jo ihan peruskansalaisella kotitietokonettaan käyttäessä. Kolmantena asiana käsiteltiin kyberstrategiaa, sen syntyä, huolehtimista sekä kehitystä. Tässä luvussa käsiteltiin myös Suomen omaa kyberturvallisuuden toimintamallia ja sen eri periaatteita.

Vertailun vuoksi käsiteltiin muutaman muunkin valtion kyberstrategioita pintapuolisesti, niihin ei tässä tutkimuksessa ollut tarvetta paneutua syvällisemmin. Viimeisenä kokonaisuutena esiteltiin itse tutkimuksen analyysi. Tähän osioon valittiin ne keskeisimmät asiat ja seikat, jotka nousivat esiin eri aineistoihin tutustuttaessa. Nämä nousivat keskeisimmiksi, tärkeiksi sekä hyödyllisiksi asioiksi lähteistä.

Nämä keskeisimmät asiat olivat kyberstrategiaan liittyvä lainsäädäntö, kyberturvallisuuskeskuksen merkitys kansallisesti, kyberturvallisuus itsessään sekä häiriötilanteiden jälkeinen palautuminen. Lopulta tutkimuksessa oli kerätty riittävät perusteet ja johtopäätökset kyettiin tekemään, kun kaikkiin edellä mainittuihin oli tutustuttu.

Tutkimuksen päätehtävä oli tutkia miten uudet uhkat vaikuttavat yhteiskunnan varautumiseen. Tutkimuksessa rajattiin uusista uhkista käsittelyyn ainoastaan kyberuhka. Kyberuhka käsitteenä avattiin tarkemmin luvuissa kaksi ja viisi. Luvussa viisi analysoitiin tutkimuksen keskeisimpiä teemoja, mitkä olivat oleellisia ja tärkeitä tutkimuksen kannalta. Tutkimus tehtiin laadullisella menetelmällä, tietoyhteiskunnan viitekehyksessä. Kybersanan tarkentaminen oli tarpeen, jotta lukija ymmärtää samat lähtökohdat kuin tutkijakin lukiessaan tutkimusta.

Tutkimuksen pääkysymyksenä oli miten yhteiskunta varautuu uusiin uhkiin. Tutkimuksessa siihen kysymykseen saatiin kattava vastaus, koska suomalainen yhteiskunta on hyvin varautunut vastaamaan kyberuhkaan. Suomelle on valmistunut ensimmäinen kansallinen kyberstrategia tammikuussa 2013. Kyberturvallisuusstrategia antaa ohjeraamin, minkä avulla yhteiskunta kykenee kontrolloimaan ja ohjaamaan yhteiskunnan kansalaisia kyberturvallisuusasioissa. Strategia ei kuitenkaan ole mikään lakikokoelma, jota on pakko noudattaa. Se on lähinnä ohjekokoelma, jonka avulla pystytään rakentamaan vahva runko kyberturvallisuuden ympärille.

Kyberturvallisuusstrategia on osoitus yhteiskunnan varautumisesta. Yhteiskuntamme ei ole muualta saadun tiedon varassa vaan kykenee vastaamaan uhkiin tarvittavalla tasolla. Yhteistyö on voimakkaasti esillä puhuttaessa varautumisesta uhkiin eli tässä tutkimuksessa kyberuhkaan. Yhteistyö on aloitettu jo ennen kyberturvallisuusstrategian laatimista. Yhteistyötä tehdään siis kaupallisten yritysten ja valtiohallinnon välillä. Suomessa on ymmärretty, ettei yhteiskuntaa kyetä turvaamaan pelkästään valtiohallinnon avulla vaan oppia on otettava ja annettava yhteiskunnan kaikille sektoreille. Yritysmaailma on pitkää ollut mukana kyberturvallisuushankkeissa jo oman

yritysturvallisuudenkin vuoksi. Valtiohallintokaan ei ole lähtenyt puhtaalta pöydältä vaan uusi perustettava kyberturvallisuuskeskus rakentuu viestintäviraston CERT-FI pohjalle.

Tutkimuksesta käy ilmi, että valtiohallinto on panostanut kyberturvallisuuden kehittämiseen jo lainsäädännön alalla. Lainsäädännössä on kyberuhkat ja niiden haittavaikutukset jo huomioitu. Laissa määritellään poikkeusolot ja niihin rinnastettavat hyökkäykset. Kyberhyökkäys on juuri sellainen hyökkäys, joka täyttää poikkeusolojen tunnusmerkit. Silloin kyetään ottamaan voimakkaampia lakeja viranomaisten käyttöön, jotta ne voivat puolustautua kybertoimintaympäristössä. Yhteiskunta siis varautuu laatimalla strategioita, parantamalla lainsäädäntöä ja tekemällä yhteistyötä. Yhteistyötä tehdään sekä kansallisella että kansainvälisellä tasolla.

Tutkimuksessa vastattiin alakysymyksiin mitä ovat uudet uhkat ja miten kyberturvallisuusstrategia huomioi kyberuhkan. Näihin kysymyksiin tutkimuksessa osittain vastattiin jo pääkysymyksen puolella, mutta yhteiskunta on määritellyt uudet uhkat tarkasti yhteiskunnan elintärkeiden toimintojen strategiassa. Tässäkin strategiassa, kuten myös kyberturvallisuusstrategiassa, on määritelty tarkkaan eri hallinnonaloittain toimet, kuinka toimitaan, mikäli yhteiskunta joutuu jonkinasteiseen poikkeustilanteeseen.

Kyberturvallisuusstrategia linjaa useassa kohdassa miten varaudutaan kyberuhkiin. Tutkimuksesta ei varsinaisesti selvinnyt mitään valmista ohjelistaa, mistä voisi lukea, mitä pitää tehdä kun huomaa joutuneensa kyberhyökkäyksen uhriksi. Kyberturvallisuuskeskus kyllä auttaa ja palvelee suurella mittakaavalla, mutta onko yksittäinen yhteiskunnan jäsen kuitenkin oman onnensa nojassa? Kyberstrategialla huolehditaan, että viranomaisilla on riittävät toimivaltuudet työskennellä kybertoimintaympäristössä. Tähän luetaan mukaan myös puolustusvoimat. Samassa asiakirjassa on vaatimuksena, että yhteiskunnassa pitää parantaa kaikkien yhteiskunnan toimijoiden kyberosaamista ja – ymmärrystä. Miten se tehdään, on vielä epäselvää? Kuten aikaisemmin jo tutkimuksessa totesin, että ihminen on heikoin lenkki kyberympäristössä. Miten parannetaan kyberturvallisuutta silloin, kun on olemassa inhimillisen erehdyksen, huolimattomuuden tai jopa välinpitämättömyyden mahdollisuus toimittaessa kybertoimintaympäristössä?

Suomella on voimakas visio olla vuonna 2016 kyberturvallisuuden kärkimaa, koska Suomella on erinomaiset valmiudet toimia tiennäyttäjänä kyberuhkien torjunnassa sekä niihin varautumisissa.

Suomi on hyvin korkeasti teknologistunut hyvinvointivaltio, josta löytyy asiantuntijoita eri aloille. Tämä edesauttaa kyberturvallisuuteen perehtymisessä.

Yhteiskuntamme elintärkeiden toimintojen turvaaminen vaatii Suomen valtiolta pitkäjänteisyyttä sekä monipuolista suorituskykyjen kehittämistä. Suomessa on tammikuussa 2013 aloitettu ensimmäinen ammattikorkeakoulupohjainen koulutusohjelma, joka keskittyy kyberturvallisuuteen. Muutamien vuosien päästä koulutuksen alkamisesta Suomeen valmistuu uusia kyberturvallisuuden asiantuntijoita, joista varmasti on hyötyä yhteiskunnan kehitykselle.

Tässä tutkimuksessa oli haastavaa, mutta myös mielenkiintoista avata kyber-käsitettä hieman enemmän. Julkaistuissa materiaaleissa oli monia eri termejä sekä merkityksiä kyber-sanalle. Terminologian yhdenmukaistaminen onkin oleellinen tekijä määriteltäessä kyberia. Laadittaessa kansallista kyberturvallisuusstrategiaa työryhmä käytti huomattavan paljon aikaa terminologiaan. Ilman yhteistä kieltä, yhteistyön tekeminen ei onnistu. Kansalliseen kyberstrategiaan on saatu terminologia päätettyä siten, että kaikki toimijaosapuolet ymmärtävät samalla tavalla mistä puhutaan.

Samankaltaista ongelmaa terminologiassa on ollut havaittavissa ympäri maailmaa, mutta kansainvälinen yhteistyö on muokannut käsitteitä siten, että puhuttaessa esimerkiksi kyberturvallisuudesta kaikki osapuolet ymmärtävät sen samalla tavalla.
Tutkimuksen tekemisen aikana mediasta saattoi olla luettavissa lähes päivittäin useaankin otteeseen kyberuhkista. Kyberuhkien lisääntyminen sekä niiden yhä kriittisempi vaikutus yhteiskunnalle on tuonut sille myös entistä enemmän mediajulkisuutta. Median kautta taas normaali kansalainen on vastaanottanut enemmän tietoa kyberuhkista. Näin ollen moni tietokoneen käyttäjä on havahtunut ja varmasti tarkastanut tietokoneensa suojauksen sekä varmistanut tarvittavien päivitysten ajan tasalla olemisen.

Median tuoman julkisuuden vuoksi on luultavammin moni tietokoneen käyttäjä ryhtynyt harkitsemaan mitä tietoja itsestään jakaa muille käyttäjille verkossa. Yksityisyyden suojaa halutaan viimeiseen asti suojella ja siksi moni kansalainen on kovin arka käyttämään tietokonetta, vaikka se onkin nykypäivän yksi arkisimmista apuvälineistä.

Median tuoma julkisuus on toisaalta etu toisaalta haitta. Etuna julkisuudelle voidaan sanoa, että lähes kaikki kansalaiset ovat tietoisia kyberuhkista ja he ovat valveutuneita kyberasioiden suhteen. Negatiivisena haittana voidaan todeta, että julkisuudella on omat varjopuolensa. Yleensä mediassa olevat otsikot ovat raflaavia ja pelottelevia. Ihmiset saavat usein vääränlaisen kuvan kyberuhkista ja koko asiaa ryhdytään pitämään pelottavana mörkönä. Totuushan on, että kyberuhka on pyörinyt tavallaan ympärillämme jo useita vuosia, mutta globalisaatio ja verkostoituminen ovat nostaneet asian voimakkaasti esille. Valitettavana haittapuolena sanottakoon, että sana kyber on kärsinyt osittain inflaation. Se ei kohta enää kiinnosta ketään.

Tavallisen kansalaisen on vaikea keskittyä ja kerätä mielenkiintoa asiaan, joka ei suoranaisesti kohdistu jokapäiväiseen elämään. Vaaditaan jokin konkreettinen tapahtuma ennen kuin normaali kadunmies ymmärtää mistä on kysymys. Tällainen normaali tapahtuma tavalliselle työssä käyvälle kansalaiselle voisi olla se, että hänen pankkitietoihinsa hakkeroitaisiin ja pankkitili tyhjennettäisiin.

Tästä mielenkiinnon puutteesta voisi vetää sellaisen johtopäätöksen, että yhteiskunta ja yritykset ovat toistaiseksi onnistuneet tehtävässään torjumaan kyberuhkia. Kyseiset tahot ovat kyenneet torjumaan yhteiskuntaa vastaan kohdistuvat kyberuhkat joten elämä on voinut jatkua normaalisti. Valitettavasti sellaista mikä ei näy ja minkä teettämä työmäärä ei juurikaan ole havaittavissa, saa aivan liian vähän arvostusta. Kyberuhkien torjunnan heikkous tai peräti puute sen sijaan huomattaisiin välittömästi.

Tässä tutkimuksessa puhutaan suomalaisesta yhteiskunnasta tietoyhteiskuntana. Nykyaikaisen tietoyhteiskunnan sujuva toiminta vaatii tietoverkoilta välttämätöntä toimintavarmuutta. Suomen valtion tulisi turvata kansalaisten tasapuolinen ja yhdenvertainen oikeusturva tietoliikenneverkoissa. Tänä päivänä suurin osa palveluista yhteiskunnassamme on sidoksissa tietoverkkoliikenteeseen. Tästä johtuen nykyaikainen tietoverkkoliikenne on heikko myös uusille uhkille, joita on todella vaikea ennakoida. Tietoverkkoliikenteeseen kohdistuu jatkuvasti hyökkäyksiä, tämän vuoksi se vaatii jatkuvaa valvontaa hyökkäyksiä vastaan. Voidaan siis sanoa, että tietoverkkoliikenteessä ei ole lainkaan rauhanaikaa.

Yhteiskunta ohjaa kansalaisiaan hoitamaan lähes kaiken mahdollisen tietoverkossa. Valtion virastot, pankit ja muut vastaavat palvelulaitokset ovat siirtäneet yksityisasiakkaiden palvelut tieto-

verkkoihin. Tästä on koitunut kustannuksia yrityksille ja eri virastoille. Kustannuksilta ei ole säästyneet myöskään kansalaiset. Palveluista joudutaan maksamaan epäsuoralla tavalla. Tietokoneet maksavat, ilman niitä on vaikea suoriutua pankkipalveluista ja muista sen kaltaisista. Tietokoneen keskimääräinen käyttöikä on neljä vuotta, sen jälkeen on taas ostettava uusi tietokone. Kuten tässä tutkimuksessa on jo puhuttu, niin tietokone tarvitsee suojautumiskeinoja. Virustorjunnat ja muut vastaavat tuotteet maksavat. Tulisiko yhteiskunnan siis myös vastata kustannuksista, joita tästä koituu ihmisille?

Suomeen on valmistunut kansallinen kyberstrategia. Se on laadittu koko yhteiskuntaa varten, ei siis pelkästään puolustusvoimille. Kyberasiat mielletään yleensä liittyvän vain puolustusvoimien työkenttään. Kansallinen kyberstrategia on yhteiskunnan ohjesääntö, jossa on laadittu toimintaohjeita ja vaihtoehtoja sille miten Suomesta saadaan kyberturvallisuuden kärkimaa. Strategia ei kuitenkaan sisällä mitään sanatarkkaa vuoropuhelua siitä, että miten erilaisissa tilanteissa tulee toimia. Se on lähinnä suuntaa antava ja siinä annetaan toimintamahdollisuus eri instansseille työskennellä itsenäisesti. Kyberstrategiassa on mietitty millaisilta kyberavaruuden toimintahäiriöiltä on osattava suojautua ja miten se tehdään.

Kenties tärkein ja merkittävin kehitysaskel on kyberturvallisuusviraston perustaminen. On hienoa, että perustetaan oma keskus, johon voidaan keskittää osaaminen ja tärkeä tietotaito. Kyberturvallisuuskeskus ryhtyy johtamaan ja hallinnoimaan kaikkia kyberturvallisuuden osa-alueita. Keskitetty johtaminen helpottaa myös kansainvälisen yhteistyön kehittämistä. Se on koordinoidumpaa sekä hallitumpaa, kun kaikki tarvittava tieto ja osaaminen ovat samassa paikkaa, saman katon alla. Kyberturvallisuuskeskusta ei tarvitse rakentaa täysin tyhjän päälle, vaan se rakennetaan Viestintäviraston CERT-Fi:n vanhalle pohjalle. On siis olemassa jo malli, jota lähdetään kehittämään eteenpäin. Kyberasiat vaativat panostamista ajallisesti ja rahallisesti. Valtion tulee sijoittaa keskuksen toimintaan, jotta sillä olisi käytössä kaikki mahdolliset resurssit. Sijoittaminen voidaan tässä tapauksessa katsoa tavallaan liikesijoittamiseksi.

Kuten olen tutkimuksessa todennut, kyberturvallisuus on kasvavaa liiketoimintaa, jossa maailmalla liikkuu satoja miljardeja euroja. Kyberturvallisuuskeskuksen tarkoitus on tutkia ja kehittää osaamistaan kyberturvallisuuden osa-alueella. Havaitut parannukset voidaan varmasti myydä kansainvälisille markkinoille tai niillä voidaan tehdä vaihtokauppaa muiden maiden kanssa. Tieto on arvokasta pääomaa ja olen varma, ettei kukaan valtio paljasta täysin omaa osaamista kyberasi-

oista. Monista asioista voidaan kuitenkin hyötyä kansallisesti, jos siitä ei ole hyötyä kaupallisilla kansainvälisillä markkinoilla.

Menestyminen kyberturvallisuuden parissa vaatii kykyä olla kokoajan ajan hermolla. Herpaantuminen voi aikaansaada pahoja takaiskuja sekä taloudellisia tappioita. Kuten tutkimuksestani käy ilmi, puolustautuminen vaatii hyökkäystaitoa. Hyökkäystaitojen opetteleminen aikaansaa varmaan pelkoa siitä, että sillä ärsytetään kyberviholinen käyttämään vastatoimia. Todennäköisesti varmaan pelätään niin kutsuttua lumipalloilmiötä, joka lähtee hallitsemattomasti vierimään koston kierteen edetessä. Uskon kuitenkin siihen, että meidän on opeteltava hyökkäämään kyberturvallisuutta vaalivia järjestelmiä vastaan. Hyökkäyksillä niistä voidaan paljastaa tietoturva-aukkoja, joita kybervastustaja voi käyttää hyväkseen. Meidän ei tarvitse kokeilla hyökkäystaitoja muita maita vastaan vaan riittää, että testaamme hyökkäyksillä omia järjestelmiämme.

Mikään suojausjärjestelmä ei kuitenkaan ole aukoton. Huolimatta siitä, että meillä olisi täydelliset järjestelmät niin niitä kuitenkin käyttävät ihmiset. Ihminen on verkkoturvallisuuden heikoin lenkki. Juuri ihminen haluaa piipahtaa työpäivän aikana facebookissa, lukea sähköpostinsa kaikkine mielenkiintoisineen liitetiedostoineen! Meidän on vaikea suojautua omalta inhimilliseltä toiminnaltamme. Internetin käyttäjän on vaikea olla objektiivinen ja suojautua kaikelta internetin tarjoamalta materiaalilta. Koulutus ja tiedottaminen ovat ainoa keino opettaa ihmisille ne perustaidot sekä käyttäytymissäännöt, joilla voimme turvallisesti toimia kyberavaruudessa. Tiedämme kuitenkin, että täydellistä suojautumisen tilaa ei koskaan saavuteta. Jos kaikki noudattaisivat sääntöjä ja ohjeita, meillä ei olisi kyberrikollisuutta tai muutakaan rikollisuutta. Nähtäväksi jää kuinka kyberturvallisuuskeskus sekä suomalainen tietotaito osaavat yhdistää voimansa ja luotsata yhteiskuntamme kyberturvallisuuden huipulle.

Tutkimuksen viitekehyksessä käytettiin tietoyhteiskuntaa. Tietoyhteiskunta kuvaa Suomen menestystä tällä hetkellä hienosti. Onko se kuitenkin terminä jo hieman vanhentunut? Teknologistuminen ja globalisaatio on ohjannut meitä suurin harppauksin eteenpäin. Mielestäni tietoyhteiskunta on muuttunut jo kyberyhteiskunnaksi. Kyberasiat ovat arkipäivää ja toimintamme on ohjautunut kehityksen myötä enemmän virtuaaliseen maailmaan. Kyberyhteiskunta ei ole kuitenkaan sama asia kuin miten se esitetään tieteiselokuva-trilogiassa Matrix. Vielä tällä hetkellä me hallitsemme kyberia, se ei ohjaa meitä. Ihminen on vielä luomakunnan ravintoketjun huipulla ja toivottavasti säilyykin siellä.

Tutkimusta tehdessä ei missään vaiheessa tullut esille selkeää ohjeistusta, miten toimitaan, mikäli laajamittainen kyberhyökkäys lamauttaisi Suomen. Kyberhyökkäys voisi kohdistua pelkästään voimalaitoksiin, kuten Stuxnet-virus Íranilaiseen ydinvoimalaan. Vastaavanlainen virus voisi teoriassa piileskellä tietoverkoissa pitkiäkin aikoja ja sitä on vaikea paljastaa, jos sellainen ei ole aktivoitunut. Aktivoituminen tapahtuu vasta, kun tietyt räätälöidyt reunaehdot täyttyvät.
Jos tällainen kyberhyökkäys lamaannuttaisi yhteiskuntamme sähköverkostoa, miten toimimme? Onko tilanne sama kuin joku vetäisi sähköpistokkeen seinästä? Sähköä varmaan saadaan jossain vaiheessa reititettyä muita kanavia pitkin, mutta miten se väliaika toimittaisiin. Varavoima ei riitä loputtomiin ja tiedonhaluisia, viluisia kansalaisia parveilee ympäriinsä. Miten hoidetaan yhteiskunnan tiedotus, jos normaalit viestintäkanavat ovat poissa pelistä sähkökatkosten vuoksi. Syntyykö paniikki ja miten tilannetta ohjataan. Tämänkaltainen esimerkki on ollut esillä eri medioissa lukuisia kertoja, mutta onko siihen olemassa valmista suunnitelmaa. Sellaista suunnitelmaa, missä on huomioitu tilanne, että mikään sähköä tarvitseva järjestelmä ei toimi. Se voisi olla katastrofaalinen ja kuinka kauan tietoyhteiskuntamme sitä kestäisi?

Tutkimuksesta kuitenkin selvisi, että huolimatta tarkemmista ohjeistuksista, Suomi on kyberturvallisuuden ammattilainen. Kyberturvallisuusstrategiassa linjattiin, että vuonna 2016 Suomi olisi johtava valtio kyberturvallisuudessa. Tätä visiota ei ole mahdotonta toteuttaa. Suomi on korkean teknologian valtio ja maamme on toistaiseksi välttynyt suuremmilta kyberhyökkäyksiltä. Suomalainen yhteiskunta on saanut rauhassa kehittyä ja valmistella omaa kybertoimintakykyään. Suomi on voinut ottaa opikseen naapurivaltioiden ja muiden valtioiden tekemistä huomioista. Suomi ei ole valtiona riippuvainen toisten antamista tiedoista, vaan kykenee tuottamaan tarvittavaa tietoa omastakin takaa. Huolestuttavampaa on yritysten kansainvälistyminen, jonka vuoksi tietopääomaa on siirtynyt ulkomaille ja se tekee osittain yhteiskunnastamme haavoittuvamman.

Kuitenkin on muistettava, ettei kybertoimintaympäristö noudata valtakunnan rajoja vaan toimii kaikkialla. Tutkimuksen lopputuloksena voin todeta, että Suomella on keinot varautua kyberuhkiin ja yhteiskuntamme on valveutunut sekä tietoinen kyberuhkien eri muodoista. Tutkimuksen perusteella voin todeta, että yhteiskunnalta puuttuu selkeät ohjeet, jotta jokainen toimija on valmis sekä ymmärtää kybertoimintaympäristön luomat haasteet. Kyberturvallisuusstrategia on kuitenkin iso edistysaskel, jolla harpataan kyberturvallisuudessa monta loikkaa eteenpäin.

LÄHTEET

Aakko Kyllikki, Nordberg Erkki, Kantolahti Erkki, Kulmala Hannes, Putkiranta Martti, Sillanpää Tuulikki, Toveri Pekka, Visakorpi Risto, Kriisiturvallisuuden käsikirja, Gummerus Kirjapaino Oy, Jyväskylä 2003

Aine Antti, Nurmi Veli-Pekka, Ossa Jaakko, Penttilä Teemu, Salmi Ilkka, Virtanen Vesa, Moderni kriisilainsäädäntö WSOYPRO oy Helsinki 2011

Alankomaat, Defensie cyber strategie, Haag 2012
http://blog.cyberwar.nl/2012/07/full-translation-of-dutch-defense-cyber.html, Viitattu 19.3.2013

Alasuutari Pentti, 2001, Laadullinen tutkimus, Jyväskylä, Gummerus, 3.painos
Ashby Ross W. 1957, An introduction to cybernetics, Chapman & Hall LTD, London

Benson Yrjö, VAHTI 15.12.2011, Kansallinen kyberturvallisuusstrategia,
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20111215VAHTIp/08_Benson.pdf, Viitattu 5.3.2013

Benson Yrjö, Kuva 4, 7.5.2012, Kansallinen kyberturvallisuusstrategia R045 7.5.2012, Turvallisuus ja puolustuskomitean sihteeristö

Candolin Catharina, Kylkirauta, Maanpuolustuksen ja johtamisen erikoislehti 1/2012, Kyberpuolustus – uusi maanpuolustuksellinen ulottuvuus,

Candolin Catharina, blogi
http://kyberturvallisuus.blogspot.fi/2011/06/kyberterrorismi-onko-sita.html, viitattu 7.3.2013

Castells Manuel, Himanen Pekka, Suomen tietoyhteiskuntamalli, Werner Söderström Osakeyhtiö, Helsinki 2001

Cebul Matthew, As-Sahab Media: "You Are Held Responsible Only for Thyself - Part 2" http://libdev.haverford.edu/gtrp/aqsi-statement/77 ja http://triceratops.brynmawr.edu/dspace/bitstream/handle/10066/7255/ASM20110603.2.pdf?sequence=1 Viitattu 7.3.2013

Chen Shay. 2007, Application Denial of Service – Is it Really That Easy? https://www.owasp.org/images/d/da/OWASP_IL_7_Application_DOS.pdf, Viitattu 6.3.2013

Clarke Richard A and Knake Robert K, Cyber war, The next threat to national security and what to do about it, New York 2010, Harper Collins Publisher

Estonia Cyber security strategy, Tallinn 2008, http://www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf Viitattu 4.3.2013

Estonian ministry of defence http://www.kaitseministeerium.ee/en/national-defense-and-society Viitattu 4.3.2013

Gibson William, Neuromancer 1984, An ace book / The Berkley Publishing Groub, New York

HE, Hallituksen esitys 44/2005 vp http://www.eduskunta.fi/valtiopaivaasiat/he+44/2005 ja http://www.finlex.fi/fi/laki/alkup/2005/20050688, Viitattu 1.4.2013

Hedemalm Gunvald, Tietoverkon perusteet, Schildts Kustannus Oy-Pagina 2000, Tummavuoren kirjapaino Oy, Vantaa

Hirsjärvi Sirkka, Remes Pirkko, Sajavaara Paula, Tutki ja kirjoita, 11.painos, Gummerus Oy, Jyväskylä 2005

Huhtanen Jarmo, Helsingin sanomat 12.10.2011, Suomi valmistautuu kybersodankäyntiin, http://www.hs.fi/kotimaa/Suomi+valmistautuu+hy%C3%B6kk%C3%A4%C3%A4m%C3%A4%C3%A4n+tietoverkoissa/a1305547028395, Viitattu 31,3.2013

Huhtinen Aki, Rantapelkonen Jari, Bumerangi 69 blogia turvallisuudesta, Johtamisen laitoksen julkaisu N:o 35, sarjassa tutkimuksia 1, Edita Oy 2006, Helsinki

Huru Jouko, Väyrynen Tarja, Kansainvälinen turvallisuus ja politiikka, Yliopistopaino 2004, Helsinki

Hyppönen Mikko 2010
http://www.talouselama.fi/uutiset/viruksesta+tuli+tasmaase/a2071896, Viitattu 7.3.1013

Härkönen Juha 2010
http://www.talouselama.fi/uutiset/viruksesta+tuli+tasmaase/a2071896, Viitattu 7.3.2013

Janczewski Lech J. and Colarik Andrew M., Cyber warfare and cyper terrorism, 2007, Hershey – New York
Jyväskylän yliopisto, haktivismi
http://kans.jyu.fi/sanasto/sanat-kansio/haktivismi, Viitattu 5.3.2013

Kajantie Sari, Kohdistetut hyökkäykset, Valtionvarainministeriön julkaisuja 6/2009, Edita Prima Oy, Helsinki

Kerttunen Mika, Kylkirauta, Maanpuolustuksen ja johtamisen erikoislehti 1/2013, Syvään kyber-strategiaan

Kramer Franklin, Starr Stuart and Wentz Larry, Cyberpower and National Security, 2009, National Defence University Press and Potomac Book, Washington, D.C.

Koukkunen Kalevi, Nykysuomen sanakirja [8]: Vierassanojen etymologinen sanakirja, useita kirjoittajia, Helsinki 1990

Lagus Antti J, Tietoturvaviikko 2009, Turvallisesti netissä, Kauppalehden erikoisliite 6.2.2009

Libicki Martin C, The mesh and the Net – Speculations on armed conflict in a time free silicon, U. S. Government Printing Office, Washington, 1994

Limnéll Jarmo, Suomen uhkakuvapolitiikka 2000-luvun alussa, Strategian laitos, Julkaisusarja 1: Strategian tutkimuksia No:29, Helsinki 2009

Lindfors Jukka, Yle, Elävä arkisto 2008
http://yle.fi/elavaarkisto/artikkelit/marsilaiset_hyokkaavat_34481.html#media=34487, Viitattu 13.3.2013

Martinez Jennifer, Kuinka näkyvä tietokoneesi on? Norton, 2013
http://www.yoursecurityresource.com/nortonpc/fi/feature/emerging_threats/computer/index.html#AuthorBio, Viitattu 31.3.2013

McClure Stuart, Scambray Joel, Kurtz George, Hakkeroinnin torjunta – Uusimmat salaisuudet ja ratkaisut, Gummerus kirjapaino Oy, 2002 Jyväskylä

Metsämuuronen Juha (toim.), Laadullisen tutkimuksen käsikirja, Gummerus Kirjapaino Oy, Jyväskylä 2006, 1.laitos, 1.painos

Norhtcutt Stephen, Novak Judy ja McLachlan Donald, Verkkomurtojen havaitseminen-analyytikon käsikirja, Gummerus kirjapaino Oy, Jyväskylä 2002

Norton, verkkorikollisuus 2013,
https://fi.norton.com/cybercrime, Viitattu 31.3.2013

Nyiri J.C., Unesco Courier, June 1997, Cyperspace: A Planetary network of people and ideas, (suomennos Petri Tapola)

Oikeusministeriö 2007
http://www.finlex.fi/fi/laki/ajantasa/2007/2007055, Viitattu 2.4.2013

Oikeusministeriö 2007
http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001, Viitattu 2.4.2013

Oikeusministeriö 2011
http://www.finlex.fi/fi/laki/ajantasa/2011/20111552, Viitattu 2.4.2013

Puheloinen Ari, Puolustusvoiman komentaja 195. Maanpuolustuskurssin avajaisissa 8.11.2010 http://www.eilen.fi/fi/972/, Viitattu 27.2.2013

Puolustusministeriö, Näkökulmia puolustuskyvyn uskottavuuteen, Toimittaja Tiina Tarvainen, Korian kirjapaino Alanko Ky, 2012

Puolustusvoimat psykologinen puolustus: http://www.puolustusvoimat.fi/wcm/ed4a8b804ce9039a97389783508f1d9d/11.6_Psykologisetoperaatiot_310512.pdf?MOD=AJPERES, Viitattu 7.3.2013

Pricewaterhousecoopers, Cyber security M&A-Decoding deals in the global cyber security industry, 2011 http://www.pwc.com/en_GX/gx/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf Viitattu 31.3.2013

Saaranen-Kauppinen Anita & Puusniekka Anna, 2006, KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_2.html, Viitattu 31.1.2013

Sallinen Anu, Sotilaallinen maanpuolustus ja yhteiskunnan elintärkeiden toimintojen turvaaminen Pohjoismaissa 2000-luvulla, Puolustusministeriön julkaisuja 2/2005, Gummerus Kirjapaino Oy, Saarijärvi 2005

Sisäasiainministeriö, tietoverkkorikollisuus http://www.intermin.fi/fi/turvallisuus/rikostorjunta/tietoverkkorikollisuus, Viitattu 5.3.2013

Stephens Bret, The Wall Street Journal, 14.4.2009, Hiroshima 2.0 http://online.wsj.com/article/SB123966785804815355.html, Viitattu 5.3.2013

Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013, Forssa Print, 2013
Suomen turvallisuus- ja puolustuspolitiikka 2004, Valtioneuvoston kanslian julkaisusarja 16/2004, Edita

Ståhle Riittamaija, Kyberstrategian voimalla, Sähkö & Tele, 1/2013
http://www.sil.fi/lehdet/st12013/Sahko_Tele1_2013.pdf, Viitattu 29.3.2013

Syrjäläinen Eija & Eronen Ari & Värri Veli-Matti, Avauksia laadullisen tutkimuksen analyysiin, Tampereen yliopistopaino Oy – Juvenes Print Tampere 2008

Talka Eira, Ruotuväki 7.2.2013, Kyberturvallisuus piiskaa tietoturvateollisuutta

Taloussanomat, "Nettiterroristit" linnaan, 2007
http://www.taloussanomat.fi/it-viikko/2007/07/08/nettiterroristit-linnaan/200716686/133, Viitattu 15.3.2013

Techterms, cyberspace
http://www.techterms.com/definition/cyberspace, Viitattu 4.3.2013

Techterms, cybercrime
http://www.techterms.com/definition/cybercrime, Viitattu 5.3.2013

Tilastokeskus 2012
http://tilastokeskus.fi/til/sutivi/2012/sutivi_2012_2012-11-07_tie_001_fi.html, Viitattu 28.3.2013

Tuomi Jouni, Sarajärvi Anneli 2009, Laadullinen tutkimus ja sisällönanalyysi, Gummerus kirjapaino Oy, Jyväskylä

Turvallisuus ja puolustusasiain komitea 2012, Kyberturvallisuus MNE7- esite
www.yhteiskunnanturvallisuus.fi, Viitattu 19.3.2013

Turvallisuus ja puolustusasian komitea 2012, Kansallinen kyberturvallisuusstrategia R045 7.5.2012

Turvallisuuspoliittinen seurantaryhmä 2008, Valtioneuvoston kanslia, julkaisusarja 8/2008, Helsinki 2008

Turvallisuusforum, Kuva 1: Yhteiskunnan turvallisuusforum Lahti 28.9.2012, Mikko Kosonen, Suomen itsenäisyyden juhlarahasto

Turvallisuusforum, Kuva 2: Yhteiskunnan turvallisuusforum Lahti 28.9.2012, Mikko Kosonen, Suomen itsenäisyyden juhlarahasto

Valtionvarainministeriö, Hallinnon turvallisuusverkkohanke TUVE, 2011 http://www.vm.fi/vm/fi/05_hankkeet/024_tuve/02_lisatietoja/tuve_esittely_112009.pdf, Viitattu 31.3.2013

Valtionvarainministeriö, ICT-varautumisen vaatimukset 2/2012 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20120925ICTvar/vahti_2_2012_NETTI_PDF.pdf, Viitattu 1.4.2013

Varto Juha, Laadullisen tutkimuksen metodologia http://arted.uiah.fi/synnyt/kirjat/varto_laadullisen_tutkimuksen_metodologia.pdf, Viitattu 1.3.2013

Viestintävirasto, CERT-FI http://www.cert.fi/, Viitattu 19.3.2013

Viestintävirasto, CERT-FI, vuosikatsaus 2012 http://www.cert.fi/tietoturvanyt/2013/03/ttn201303141219.html, Viitattu 28.3.2013

Viestintävirasto, Signaali 4/2011, Kansallinen kyberturvallisuusstrategia etenee http://www.epaper.fi/reader/?issue=24657;fd2ba8acc233cc698c57e13e156dec0a;18, Viitattu 19.3.2013

Viestintävirasto, Tietoturvaopas 2008, Haittaohjelmat http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html, Viitattu 6.3.2013

Vilkka Hanna, 2005, Tutki ja kehitä, Keuruu, Kustannusosakeyhtiö Tammi

Virta Jami, Johtamisen laitoksen tutkimusohje, Julkaisusarja 1, Tutkimuksia Nro 36, Edita Prima Oy, Helsinki

Vuori Juha 2005, Turvallisuudesta uhkantorjuntaan, Kosmopolis - Vol.35:4/2005

Yhdysvallat, Cyberspace policy review 2009
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, Viitattu 19.3.2013

YETTS, Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös 23.11.2006, Kirjapaino Keili Oy, 2006

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010,Vammalan kirjapaino, 2011

YLE MOT-OHJELMA, Suomi polvilleen 15 minuutissa 11.3.2013

Yleisradio, uutiset – Puolustusvoimat rakentaa kiireesti kykyä vastata verkkohyökkäyksiin, 29.10.2011
http://areena.yle.fi/tv/1338602, Viitattu 31.3.2013